Parlament Österreich

Ausschuss für innere Angelegenheiten

Auszugsweise Darstellung

verfasst von der Abteilung 1.4/2.4 – Stenographische Protokolle

28. Sitzung

Mittwoch, 19. Juni 2024

XXVII. Gesetzgebungsperiode

TOP 1

Antrag der Abgeordneten Dr. Christian Stocker, David Stögmüller, Kolleginnen und Kollegen betreffend ein Bundesgesetz, mit dem ein Netz- und Informationssystemsicherheitsgesetz 2024 erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden (4129/A)

13.04 Uhr – 13.48 Uhr

Nationalratssaal

www.parlament.gv.at

Auszugsweise Darstellung

Ausschuss für innere Angelegenheiten – XXVII. GP 19. Juni 2024 28. Sitzung / 2

Beginn des öffentlichen Teils von TOP 1: 13.04 Uhr

TOP 1

Antrag der Abgeordneten Dr. Christian Stocker, David Stögmüller, Kolleginnen und Kollegen betreffend ein Bundesgesetz, mit dem ein Netz- und Informationssystemsicherheitsgesetz 2024 erlassen wird und das Telekommunikationsgesetz 2021 und das Gesundheitstelematikgesetz 2012 geändert werden (4129/A)

Obmann Dr. Christian Stocker geht in die Tagesordnung ein und kommt sogleich zu Tagesordnungspunkt 1.

Nach der Berichterstattung durch Berichterstatterin Himmelbauer, BSc, und einer kurzen Sitzungsunterbrechung zwecks Einlasses der Experten sowie allfälliger Zuhörer:innen dankt der Obmann den Experten für ihr Kommen.

Sodann leitet der Obmann –nach Mitteilungen hinsichtlich der Redeordnung – zur Debatte über und erteilt Bundesminister Karner für eine einleitende Stellungnahme das Wort.

Einleitung des Bundesministers für Inneres Mag. Gerhard Karner

Bundesminister für Inneres Mag. Gerhard Karner: Vielen herzlichen Dank, sehr geehrter Herr Vorsitzender! Geschätzte Damen und Herren Abgeordnete! Geschätzte Mitarbeiterinnen und Mitarbeiter, Experten! Ich möchte mit einem großen Dank beginnen. Ich bedanke mich, dass heute das sogenannte NIS2-Gesetz auf der Tagesordnung des Innenausschusses ist und möchte mich vor allem bei jenen dafür bedanken, die die intensive Vorarbeit für dieses Gesetzesvorhaben geleistet haben.

Viele Expertinnen und Experten aus dem Bereich des Innenressorts, aber auch außerhalb, aus dem Bereich der Industriellenvereinigung, der Wirtschaftskammer, von

vielen zivilgesellschaftlichen Organisationen, haben ihren Beitrag dazu geleistet, dass wir jetzt eine Grundlage haben, um im Ausschuss darüber zu beraten, zu beschließen, zu diskutieren, damit dieses NIS2-Gesetz auch in Österreich umgesetzt werden kann.

Sie wissen, dass im Jänner 2023 die sogenannte NIS2-Richtlinie auf europäischer Ebene beschlossen wurde, parallel dazu auch massiv auf nationaler Ebene Beratungen stattgefunden haben. Warum? – Weil es einfach notwendig ist, dass wir in diesem Bereich Netzsicherheit, Cybersecurity, Cybercrime auch national entsprechende Fortschritte machen.

Wenn Sie die polizeiliche Anzeigenstatistik lesen, dann wissen Sie, dass der Bereich Cybercrime einer jener Bereiche ist, der am stärksten im Steigen begriffen ist. Dieser Teil, Netzsicherheit, ist eben ein wesentlicher Teil, in dem wir auch Erfolge erzielen müssen. Daher vielen Dank, dass sich an diesem Prozess, der vor eineinhalb Jahren begonnen hat, viele beteiligt haben.

Wie gesagt, es gab viele Beteiligte, Stakeholder sagt man auf neudeutsch, bei der Erarbeitung dieser Gesetzesvorlage, mit dem klaren Ziel dieser europäischen Richtlinie, die Widerstandsfähigkeit im Cyberbereich zu erhöhen, die Reaktionszeit auf Cyberangriffe zu verkürzen und auch möglichst –möglichst! – einheitliche Standards festzulegen.

Wir wissen auch, es wird eben viel, viel mehr Organisationen, Unternehmen, Gebietskörperschaften des öffentlichen Rechts und Vereine betreffen, als das bisher der Fall war. Von NIS1 waren bisher rund 100 Organisationen betroffen, in Zukunft werden es an die 3 bis 4 000 sein, die letztendlich davon betroffen sind. Diese Richtlinie, und das ist das Ziel dahinter und das ist auch unser Ziel, bedeutet Schutz und Sicherheit aber auch – und das muss man auch in aller Offenheit und Ehrlichkeit sagen und das haben wir auch in den vielen Veranstaltungen gesagt – Aufwand und Arbeit für die Betroffenen.

Wie gesagt, wir haben daher bereits vor eineinhalb Jahren einen Prozess gestartet, wo wir vor allem mit Expertinnen und Experten aus dem Bundeskanzleramt, aus dem Innenministerium, gemeinsam mit der Industriellenvereinigung, mit der Wirtschaftskammer viele Informationsveranstaltungen durchgeführt haben, in welche Richtung dieses Gesetz gehen soll, immer mit der klaren Vorgabe, immer mit dem klaren Ziel Beraten statt strafen und vor allem auch, kein sogenanntes Gold Plating durchzuführen, was die Umsetzung der Richtlinie betrifft, damit auch die betroffenen Organisationen, Unternehmen, Vereine dieses Gesetz so annehmen, wie die Zielsetzung dahinter ist, nämlich es für sie selbst zu verwenden, um für Schutz und Sicherheit in der eigenen Organisation zu sorgen.

Daher noch einmal: Vielen Dank für diese intensive Vorbereitung, für diesen intensiven Diskussionsprozess, letztendlich noch bevor eine Begutachtung stattgefunden hat – wie gesagt, mit vielen Beteiligten. Mein Dank gilt auch dem Koalitionspartner für die intensiven Gespräche, der Industriellenvereinigung, der Wirtschaftskammer, den vielen Beteiligten, den Experten, die zu Rate gezogen worden sind, damit wir auf nationaler Ebene dieses Gesetz bis Ende des Jahres EU-richtlinienkonform beschließen und umsetzen können, weil das einfach im Sinne der Betroffenen ist, die in Zukunft dieses Gesetz letztendlich zu vollziehen haben. – Vielen herzlichen Dank!

Obmann Dr. Christian Stocker bedankt sich beim Innenminister für dessen einleitende Worte und leitet zu den Eingangsstatements der Experten über.

Eingangsstatements der Experten

Mag. Otmar Lendl: Sehr geehrte Damen und Herren! Vielen Dank für die Gelegenheit, hier als Techniker Feedback zu geben und zu erklären, was das neue Gesetz aus meiner Sicht und aus der Sicht der Leute, die die letzten Jahre schon mit dem Thema gearbeitet haben, heißt.

Punkt eins: Brauchen wir das Thema überhaupt? – Die IT ist inzwischen zu einem wesentlichen Teil unseres Lebens geworden. Gibt es dort Ausfälle, trifft das uns als Gesellschaft. Das heißt, wir müssen das Thema inzwischen so gut behandeln wie auch Brandschutz, Verkehrssicherheit und andere Themen, bei denen wir im Sinne der gesamtstaatlichen Sicherheit der Menschen, der Gesellschaft regulierend eingreifen müssen und gewisse Mindeststandards vorgeben müssen.

Es geht bei NIS nicht rein um die böswilligen Akteure. Es geht jetzt nicht rein um Cybercrimeverhinderung, sondern es geht darum, dass wir in unseren Firmen, unseren Behörden und anderen Organisationen einen IT-Betrieb brauchen, auf den wir uns verlassen können – weil der unsere Gesellschaft trägt. Das heißt, es geht um sichere Betriebsführung, sowohl in der normalen Tätigkeit der IT, als auch in Bezug auf die Abwehr von verschiedenen Angriffen von außen. Wir haben mit der NIS1 ein gutes Fundament. Wir haben jetzt jahrelange Erfahrung in der Zusammenarbeit zwischen den Stakeholdern im Staat – Innenministerium, Kanzleramt, Verteidigung, Außenministerium – und externen Leuten. Wir haben auch eine sehr gute Zusammenarbeit zwischen den Behörden, die dieses Gesetz exekutieren, und denen, die ihm unterworfen sind, geschaffen.

In vielen Fällen haben es die Firmen geschafft, diese Energie, die da von oben gekommen ist, diesen regulatorischen Druck zu nehmen und in einem Judo-Move quasi zu sagen: Hey, das wissen wir eh, dass wir das schon längst hätten machen sollen, jetzt haben wir den Anlass und die Motivation, jetzt ziehen wir es wirklich durch! Das heißt, soviel auch manchmal darüber geschimpft wurde, dass das Aufwand bedeutet, in vielen Bereichen haben die Sicherheitsverantwortlichen gewusst, das müssen wir eh schon machen. Das ist eh schon längst auf unserem Speisezettel und jetzt machen wir es wirklich, jetzt ziehen wir es durch, jetzt werden die Projekte endlich möglich.

Daher die Frage: Sind die Maßnahmen für die Betroffenen machbar? Da fragen wir einmal diejenigen Firmen, die jetzt schon darunterfallen, nach NIS1. – Ja, das haben

sie geschafft. Wir haben ein klare Geschichte, einen genauen track record dafür. Ja, NIS umzusetzen ist machbar. Für einige, die jetzt neu mit NIS2 darunterfallen, wird das initial ein bisschen ein Schnaufen geben. Das ist nicht einfach für sie, das ist Aufwand, wird aber der Anlass sein, das Thema endlich systematisch anzugehen und abzuhandeln. Das wird in vielen Firmen einen relativ starken Reifeprozess auslösen.

Wir haben leider im aktuellen Gesetz auch ein paar Treffer von Firmen dabei, die eigentlich nicht hineinfallen, aber die laut EU-Vorgaben darunterfallen sollten. Ich bin aber sehr optimistisch, dass wir da einen Weg finden, das für diese möglichst aufwandssinnvoll abzuhandeln. Für alle gilt aber: Dieses Gesetz ist ein Anlass dafür, sich Gedanken zu machen, wie sehr ihre IT relevant ist, welche Gefahren dafür bestehen, sowohl von böswilligen Tätern als auch durch einfache Betriebsfehler, Ausfälle, oder einfach nur äußere Einflüsse, und darauf basierend dann Risikomaßnahmen zu setzen, um die Firma und Organisation in ihrer Betriebssicherheit zu stärken.

Der Text selbst ist aus technischer Sicht relativ klar aus Brüssel vorgegeben worden. Das Ganze gab uns nur überschaubar viel Gestaltungsspielraum in Österreich. Wir konnten daher einiges von dem guten Feedback aus den Stellungnahmen nicht aufnehmen, weil einfach das Korsett aus Brüssel zu eng dafür war. Die Textvorgaben aus Brüssel waren auch nicht immer von der besten Qualität. Ich hätte mir gewünscht, dass wir da und dort ein bisschen mutiger sind und den Text besser formulieren als in den EU-Vorgaben, die als Beispiel für uns vorgelegen sind.

Wir hätten auch da und dort ein bisschen mehr Mut haben können, gestalterisch einzugreifen und zum Beispiel im Bereich Informationssharing die I-Secs, die vorkommen –§ 36, glaube ich, ist das –, ein bisschen klarer auszugestalten und uns besser zu überlegen, wie wir das Ganze hier in Österreich mit Leben erfüllen können, weil wir schon gute Vorarbeiten haben, auf die wir aufbauen können.

Leider hatten wir auch nur eine Runde Feedback aus der Gesellschaft. Es wäre deutlich schöner gewesen, hätten wir schon vor einem Jahr breiter gesellschaftlich diskutiert, wie wir das Thema in Österreich aufziehen sollen. Es gab da schon einiges an guten Gesprächen im Bereich der CSP – der Cybersecurityplattform –, vor allem, was die Risikomanagementmaßnahmen angeht. Ich glaube, wir sollten dieses Forum auch nutzen, um früher schon über den Gesetzestext und die Strukturen, die da kommen werden, zu reden.

Die Architektur: Die Überführung der Agenden ins BMI ist ein Weg, das zu machen. Wenn ich mit meinen Kollegen aus den anderen EU-Staaten spreche, sehe ich, wie das Thema dort auf eine weite, breite Art aufgestellt ist. Es gibt da keinen europäischen Standard, wie das Thema angelegt ist. Es gibt das zum Teil unter dem Premierminister – Beispiel Belgien –, Innenressort, Finanz, National Security Authority, Militär, Nachrichtendienst – Beispiel Dänemark –, Wirtschaftsministerium, Digitalisierungsministerium. Es ist wirklich breit. Manchmal ist es alles im Ministerium, manchmal ist es quasi outgesourct in ein Amt – siehe BSI in Deutschland. Manchmal ist das alles in eine Einheit verpackt, ein National Cybersecurity Center. Manchmal ist es mehr aufgespalten, sektoral oder auch zwischen Hilfe und Regulierung. Es gibt wie gesagt keine klare Vorgabe aus anderen Staaten: Das ist der beste Weg, wie man so etwas machen muss. Daher ist die Entscheidung, wie das in Österreich aufgestellt werden soll, aus meinem Blickwinkel, aus dem technischen Blickwinkel, eine rein politische Entscheidung und keine technische Entscheidung.

Aus technischer Sicht hat es wiederum Vor- und Nachteile, alles ins BMI zu geben. Wir haben alles in einer Hand, aus einem Griff – und die Erfahrung hat gezeigt, dass wir mit der aktuellen Mannschaft im BMI extrem gut zusammenarbeiten können. Also ich habe aus Sicht des Computernotfallteams keine Bedenken, dass das Ganze im BMI landet. Wir müssen aber ein bisschen aufpassen: Es gibt da Zielkonflikte. Beispiel: Aus der Sicht der Cybersicherheit ist es ganz wichtig, dass Sicherheitslücken effizient und schnell geschlossen werden, während es, wie wir gerade in den letzten Tagen gehört haben, vielleicht in anderen Bereichen die Tendenz dazu gibt, Schwachstellen zu

nutzen, um die Arbeit der Polizei zu vereinfachen. Diesen Konflikt müssen wir auflösen.

Es muss uns klar sein, was für die NIS-Behörde das obere Ziel ist. Wir haben bei sowas auch immer das Thema Hilfestellung versus Aufsicht. Das BMI ist laut Entwurf die Aufsichtsbehörde für die NIS-unterworfenen Firmen. Gleichzeitig soll aber auch über die Notfallteams und das BMI Hilfe an die Betroffenen gegeben werden. Es ist daher wichtig, dass wir uns klar werden, dass wir das organisatorisch intern trennen müssen, dass nicht aus dem Hilfeanruf wird: Aber du Böser hast hier gegen das Gesetz verstoßen! Das muss man schön sauber trennen.

Obmann Dr. Christian Stocker weist den Experten darauf hin, dass dessen Redezeit bereits überschritten sei, und bittet ihn, zusammenfassend zum Schluss zu kommen.

Mag. Otmar Lendl: Zusammenfassend: Ich glaube, wir brauchen das. Wir brauchen das vor allem, um die Strukturen aufzubauen. Die alten aus NIS1 reichen nicht mehr ganz. Ich glaube, wir sollten das durchziehen. – Danke.

Sebastian Kneidinger: Sehr geehrte Damen und Herren! Im Namen der unabhängigen Datenschutz-NGO Epicenter Works bedanke ich mich herzlich für die Einladung.

Wie einige prominente Fälle in den letzten Jahren gezeigt haben, besteht in unserem Land ein dringender Nachholbedarf in Fragen der Cybersicherheit. Ein wichtiger Baustein dazu ist sicherlich die Umsetzung der NIS2-Richtlinie, aber die Vorteile dieser Richtlinie können nur mit einer durchdachten und zielgerichteten Umsetzung realisiert werden. Der vorliegende Entwurf scheitert aus unserer Sicht an diesen Anforderungen und sollte deshalb auch grundlegend überarbeitet werden. Die Kritik von uns, aber auch von anderen Stakeholdern aus dem Begutachtungsverfahren kann man im Wesentlichen auf vier Punkte reduzieren, zu denen ich später noch mehr ausführen werde:

Erstens – das ist der wichtigste Punkt –: Konstruktionsfehler; das ist die Ausgestaltung der nationalen Cybersicherheitsbehörde, die erachten wir als nicht geglückt.

Zweitens: Es gibt überschießende Kompetenzen und Befugnisse beim Innenministerium.

Drittens: Wir sehen eine verpasste Chance beim Schutz der verantwortungsvollen Offenlegung von Schwachstellen.

Viertens: Wir sehen überschießende Datenverarbeitungs- und Übermittlungskompetenzen.

Zum ersten Punkt, dem Konstruktionsfehler der nationalen Cybersicherheitsbehörde: Wie mein Vorredner schon angemerkt hat, bringt die Ansiedlung im Innenministerium zwangsläufig auch einen Zielkonflikt, denn das für ein gutes Zusammenarbeiten von betroffenen Unternehmen und Sicherheitsforschung notwendige Vertrauen wird immer mit der Befürchtung der individuellen Strafverfolgung und allgemein Gefahrenabwehr zu kämpfen haben.

Strafverfolgung beziehungsweise allgemeine Gefahrenabwehr wird beim BMI immer Vorrang vor der allgemeinen IT-Sicherheit des Landes haben. Einen solchen Zielkonflikt sehen aber nicht nur wir, sondern zum Beispiel auch der ehemalige CIO des Saarlandes im Rahmen der öffentlichen Anhörung im deutschen Bundestag.

Wir möchten auch darauf hinweisen, dass bereits bisher mangelnde Personalausstattung bestanden hat. Es ist kein Geheimnis, dass der öffentliche Dienst Schwierigkeiten hat, IT-Spezialisten als Mitarbeiter zu gewinnen. Dieses Problem hat auch der Rechnungshof erst letzte Woche wieder kritisiert. Das mag an den Gehältern liegen, die in der Privatwirtschaft viel höher sind. Wir wissen auch, dass es da erste Bemühungen gegeben hat; aber mit der vorliegenden Konstruktion bleibt auch die kulturelle Frage – konkret: Gute Hacker werden nicht im Innenministerium arbeiten,

in einer unabhängigen Cybersicherheitsbehörde aber sehr wohl. Unsere Aufforderung ist: Lernen wir von unseren Erfolgen und nehmen uns die Konstruktion ähnlich der KommAustria und der RTR GmbH als Vorbild!

Als Nächstes sehen wir eine mangelnde Einbindung von Wissenschaft, Zivilgesellschaft und Wirtschaft. Wir haben viel Expertise zur IT-Sicherheit in Österreich, aber anstatt diese Akteure einzubeziehen, finden sie sich mit kritischen Stellungnahmen im Begutachtungsverfahren. Cybersecurity ist eine Gemeinschaftsleistung, gerade angesichts hybrider Bedrohungsszenarien, Stichwort Russland. Als positives Beispiel wollen wir Italien nennen. Es hat ein Technical Scientific Advisory Board eingerichtet, also ein Beratungsgremium für die nationale Cybersicherheitsbehörde, bestehend aus Vertretern von Wissenschaft, Wirtschaft und Interessenvertretung der IT-Sicherheitsexperten.

Der Konstruktionsfehler wird auch im europäischen Vergleich deutlich. Die führenden Staaten setzen auf andere Konstruktionen. In Deutschland gibt es mit dem Bundesamt für Sicherheit in der Informationstechnik ein eigenes Amt, in Litauen sind diese Kompetenzen beim Verteidigungsministerium. Unsere Empfehlung daher: eine unabhängige Stelle nach dem Vorbild der KommAustria zu schaffen. Uns ist wichtig, hinzuweisen: Das soll keine Kritik an den jeweiligen Vertretern aus dem Innenministerium sein, sondern wir sehen hier einen inhärenten, systemischen Zielkonflikt, mit dem sich auch andere Akteure in Europa schwertun.

Zweiter Punkt: die überschießenden Kompetenzen und Befugnisse der neuen Cybersicherheitsbehörde beim Innenministerium. Wir nennen hier zum Beispiel die alleinige Ernennung des nationalen CIR durch das Innenministerium. Das nationale CIR, derzeit cert.at, ist die zentrale Anlaufstelle für Cybernotfälle in Österreich und hat daher auch eine herausragende Stellung. Es ist wichtig, dass die Ernennung des CIR gemeinsam mit anderen Ressorts zu erfolgen hat. Nur, wenn die Stakeholder in Österreich Vertrauen zu dieser Stelle haben, kann sie auch funktionieren.

Weiters sehen wir auch die Einsichts- und Kontrollrechte als überschießend. Diese neuen Kompetenzen sind ausufernd und viel zu ungenau determiniert. Der derzeit vorliegende Entwurf im Initiativantrag brachte zwar gewisse Verbesserungen, aber die grundlegende Kritik bleibt aufrecht. Das wurde auch in unterschiedlichen Stellungnahmen im Begutachtungsverfahren kritisiert. Neben uns kritisiert etwa auch die Örak den Umfang als „unklar“, sieht ihn „angesichts der potentiellen Eingriffsmöglichkeiten in sensible Unternehmensbereiche jedenfalls“ als „problematisch“ und im vorliegenden Wortlaut auch als unverhältnismäßig. Wie gesagt, uns ist bewusst, dass es hier schon Verbesserungen gegeben hat.

Dritter Punkt: Das ist die verpasste Chance, die Thematik der Absicherung von Responsible Disclosure. Mit § 11 des NIS2-Gesetzes wird zwar dem Wortlaut nach den Vorgaben der NIS2-Richlinie entsprochen. Dem Ziel und Zweck der Bestimmung – nämlich die koordinierte Offenlegung von Schwachstellen zu erleichtern – wird diese Minimalvariante der Umsetzung jedoch nicht gerecht. In Österreich ist es immer noch so, dass der moralisch richtige Umgang mit Sicherheitslücken – nämlich das Melden an die Verantwortlichen – nicht belohnt, sondern viel eher bestraft wird. In anderen Ländern gibt es schon längst einen sicheren Rechtsrahmen für gemeldete Schwachstellen. Auch die EU-Behörde für Netzwerksicherheit, die Enisa, empfiehlt klar, Ethical Hacker abzusichern. Trotz des Erlasses im Bundesministerium für Justiz fehlt eine solche Absicherung in Österreich und es sollte daher dringend eine Anpassung der straf- und datenschutzrechtlichen Bestimmungen erfolgen.

Vierter und letzter Punkt sind die weitreichenden Datenverarbeitungs- und Übermittlungsmöglichkeiten. Zum Beispiel kennt § 17 eine Verpflichtung des BMI zum Betrieb von IKT-Lösungen zur Früherkennung von Cyberbedrohungen. Wesentliche Einrichtungen können daran teilnehmen, und angesichts der fraglichen IT-Sicherheitssituation werden wohl auch viele Unternehmen daran teilnehmen wollen. Wir sehen aber die Gefahr einer anlasslosen Massenüberwachung aufgrund der gesetzlichen Ausgestaltung.

Weiters sieht z. B. § 42 vor, dass eine Datenverarbeitung nicht nur zu Zwecken der Umsetzung des NIS2-Gesetzes erfolgen darf, sondern auch „zum Schutz vor und der Abwehr von Gefahren für die öffentliche Sicherheit“. Das heißt, der Zielkonflikt, den wir auf systemischer Ebene aufgezeigt haben, findet sich hier noch mal auf Datenverarbeitungsebene. § 43 kennt eine ungenau determinierte Übermittlungsmöglichkeit von personenbezogenen Daten an andere in- und ausländische Behörden oder Stellen. Wir und viele andere Stakeholder orten in der ungenauen Bestimmung die Gefahr des Abflusses von personenbezogenen Daten oder von Geschäfts- oder Betriebsgeheimnissen. Auch wenn mit dem vorliegenden Entwurf im Initiativantrag minimale Verbesserungen durch das Auflisten der Datenkategorien erfolgt sind, sind die genannten Bestimmungen aus Datenschutzsicht weiterhin klar abzulehnen.

Um zum Abschluss zu kommen und die 8 Minuten Redezeit zu wahren: Aus diesen Überlegungen heraus empfehlen wir die Neuausarbeitung des Gesetzes unter breiter Einbindung aller relevanten Stakeholder in Österreich aus Forschung, Zivilgesellschaft und Wirtschaft. Es geht hier nicht nur um ein abstraktes oder theoretisches Thema. Bei IT-Sicherheit geht es um den Schutz von Krankenhäusern, der öffentlichen Verwaltung, Schulen, der Privatsphäre von allen Menschen in unserem Land und auch um den Schutz der Wirtschaft vor Angriffen aus dem Ausland.

Das Thema hat es verdient, ernsthafter und ehrlicher behandelt zu werden, als dieser Entwurf es probiert hat. – Vielen Dank.

Obmann Dr. Christian Stocker dankt dem Redner für dessen Ausführungen, weist auf die vorgesehene Redezeit von 2,5 Minuten hin und leitet zur ersten Fragerunde der Abgeordneten über.

Fragerunde der Fraktionen

Abgeordnete Eva-Maria Himmelbauer, BSc (ÖVP): Herr Vorsitzender! Herr Bundesminister! Danke den Herren Experten für ihre Stellungnahmen! Die Bedeutung

und die Notwendigkeit dieser Richtlinie und auch der gesetzlichen Umsetzung haben Sie, glaube ich, stark betont; das kann ich auch nur bekräftigen. NIS1 war durchaus auch durch einen sehr starken und sehr intensiven Stakeholderprozess im Vorfeld geprägt. Das empfinde ich da aber gleichermaßen, auch wenn die letzte Wortmeldung dies nicht bekräftigt.

Aus meiner Sicht und auch aus vielen Gesprächen, die ich im Vorfeld geführt habe, ist es aber durchaus sehr gut angenommen worden, dass hier im Vorfeld bereits sehr intensive Kontakte gepflegt worden sind und auch hinsichtlich der Ausgestaltung gesprochen worden ist. Wir wollen alle die Resilienz unserer Wirtschaftsakteure – von Privaten, öffentlicher Verwaltung und Wirtschaft insgesamt – fördern, und ich glaube, es ist in unserem Sinne, das Sicherheitsniveau insgesamt zu heben.

Ein paar Fragen zur Umsetzung an die Herren Experten: Vielleicht können Sie uns kurz aufschlüsseln, was bis auf die, die davon betroffen sind, der Unterschied zur NIS1 ist. Gibt es auch in der Maßnahmenumsetzung konkrete Unterschiede? Meine Frage geht in Richtung Bürokratie- und vielleicht auch Kostenabschätzung für Unternehmen, weil es jetzt viel mehr mittlere Unternehmen sind – und wenn man die Lieferkette vielleicht auch hinzuzieht, Kleinstunternehmen, die vielleicht auch davon betroffen sind. Wir haben in den letzten Wochen gerade sehr intensiv über Bürokratieabbau gesprochen. Man merkt bei den Stellungnahmen: Es ist sehr viel aus der Sozialwirtschaft und aus dem Gesundheitsbereich gekommen. Inwieweit wurden die Anliegen und Befürchtungen vielleicht auch wahrgenommen und umgesetzt? Ich weiß persönlich aus dem Pflegebereich, dass es eine große Definitionsfrage war: Ab wann ist Pflege überhaupt auch als kritischer Bereich relevant?

An das Ministerium hinsichtlich der Verordnungen: Es gibt ja durchaus einige Verordnungsermächtigungen in dem Gesetz, die vor allem eine Präzisierung vorsehen. Das ist für die Unternehmen, die jetzt auch in der Umsetzungsphase sind, sehr relevant. Wann werden die kommen?

Betreffend diese Plattform, die da ja schon genutzt worden ist, um sich auszutauschen – weil auch von Expertenseite der Vorschlag kam –: Ich gehe davon aus, die wird ja auch in der weiteren Ausgestaltung der Verordnungsentwürfe weiterhin eingebunden sein.

Hinsichtlich der Umsetzungsfrist bis 1. Juni 2025, die jetzt im Gesetz vorgesehen ist, möchte ich noch positiv hervorheben: Es ist natürlich sehr viel Arbeit, die da jetzt reingesteckt werden muss, auch von den Unternehmen. Die Selbstmeldung ist für viele noch ein bisschen ein Fragezeichen: Falle ich darunter oder nicht? Es gibt den Akteuren jetzt durchaus die notwendige Zeit, sich bestmöglich vorzubereiten, das möchte ich auch noch betonen. – Danke schön.

Abgeordnete Katharina Kucharowits (SPÖ): Herr Vorsitzender! Herr Bundesminister! Geschätzte Experten, herzlichen Dank für Ihre Inputs und Ihre Sichtweise! Ich möchte vorwegschicken, dass es natürlich ganz klar zentral wäre, hohe Cybersicherheitskriterien beziehungsweise -regelungen auf die Füße gestellt zu bekommen, und dass das für uns natürlich richtig und wichtig ist. Ich glaube, das steht gänzlich außer Frage. Wir müssen als Staat, aber auch als EU in diesem Bereich einfach resistent und resilient werden, und ich glaube, das wäre auch das eigentliche Ziel.

Mit NIS1 ist ein Schritt gesetzt worden und NIS2 ist, wie Sie richtig gesagt haben, Herr Bundesminister, eigentlich seit Dezember 2022 fertig und müsste am 18. Oktober 2024 national implementiert werden. Sie haben sich aber sehr lange Zeit gelassen. Sie haben – das möchte ich vorwegschicken – das Parlament in keinster Weise in der Tiefe eingebunden, vielleicht die Regierungsfraktionen, aber dezidiert nicht die Oppositionsfraktionen. Auch die Zivilgesellschaft – Sie haben das jetzt auch gerade gehört – hat sich nicht in dem Umfang eingebunden gefühlt, wie Sie das in Ihrem Eingangsstatement gesagt haben.

Das sind ein paar Gründe, und ich finde auch, dass die Experten, ehrlich gesagt, ein paar Fragen aufwerfen.

Die erste Frage an Sie, Herr Bundesminister, ist: Wieso haben Sie dieses Superministerium kreiert? Es braucht mit Sicherheit 500 Fachkräfte. Die Experten sind darauf eingegangen, dass diese Fachkräfte womöglich nicht zur Verfügung stehen werden. Wie würden Sie das dementsprechend gewährleisten?

Das Zweite ist: Es würde mich interessieren, wieso Sie – das ist vom Experten Kneidinger genannt worden – die sogenannten gemeldeten Schwachstellen nicht gleich ins Gesetz mit eingebunden haben. Wir hatten ja auch erst ein Thema. Wieso fehlt das? Andere Länder haben das dezidiert schon umgesetzt und auch implementiert.

Dann zwei Fragen an die Experten: Sie haben von der überbordenden Datenverarbeitung und -weiterverarbeitung an sich gesprochen. Sehen Sie die Vorratsdatenspeicherung über die Hintertür in dem Gesetz verankert? Das würde mich von Ihnen beiden interessieren.

Herr Mag. Lendl, Sie haben auch ausgeführt, dass es zentral wäre, das jetzt umzusetzen, haben aber, wie auch Herr Kneidinger, den Zielkonflikt – es ist bei einer Behörde im Innenressort angesiedelt – kritisiert und kritisch angemerkt. Deshalb meine Frage: Sind Sie wirklich der Meinung, dass das Bundesministerium für Inneres die geeignete Behörde ist, und glauben Sie auch, dass dieser Zielkonflikt bewältigt werden kann und dass dieser Widerspruch nicht besteht?

Herr Bundesminister, ich frage jetzt noch einmal: Sie haben sich wirklich ein Gesetz geschaffen oder möchten sich ein Gesetz schaffen, das wirklich unglaublich überbordend ist, nämlich auch, was Weisungen anbelangt. Das gab es in der Republik noch nie. Es ist auch so, dass Sie ganz klar Kompetenzzuständigkeiten überschreiten, nämlich jene der Länder und dezidiert auch der Gemeinden. Die Frage ist: Wieso schaffen Sie das? Wieso haben Sie sich für diesen Weg entschieden und es nicht wie

beispielsweise andere Länder gemacht, wo explizit darauf hingewiesen wurde, dass mehrere Ministerien involviert werden, ein Bundesamt installiert werden würde? Wir haben ja auch schon Beispiele bei anderen Dingen, die wir in Österreich geregelt haben, etwa die KommAustria. Die Frage ist, warum Sie das dezidiert nicht gemacht haben.

Für uns ist das Gesetz, das hier am Tisch liegt, eines, das wirklich überbordend ist. Die parlamentarische Kontrolle ist in keinster Weise gewährleistet. Warum? – Weil die Komplexität enorm ist und damit das Interpellationsrecht nicht erfüllt werden kann und womöglich auch missachtet würde.

Obmann Dr. Christian Stocker weist die Fragestellerin darauf hin, dass die Fragezeit überschritten ist.

Abgeordnete Katharina Kucharowits (SPÖ): Ja, ich komme schon zum Schluss: Die Sozialdemokratie wird diesem Gesetz aufgrund der kritischen Anmerkungen, die ich soeben getätigt habe, definitiv nicht zustimmen.

Obmann Dr. Christian Stocker weist darauf hin, dass in diesem Teil des Tagesordnungspunktes vorgesehen ist, ein Hearing mit den Experten durchzuführen, und bittet darum, die Zeit dafür zu verwenden, Fragen an die Experten zu richten. Eine Wortmeldung seitens des Ministeriums sei nicht vorgesehen, diese könnte in der Debatte danach stattfinden.

Abgeordneter Mag. Hannes Amesbauer, BA (FPÖ): Herr Vorsitzender! Danke auch an die beiden Experten für den Überblick und für die Beschäftigung mit der doch recht komplexen Materie und die Analyse, die Sie uns dargeboten haben.

Was wir gehört haben – und zwar von beiden Experten –, bestätigt mich schon in der Kritik, die wir an diesem ganzen Entwurf, der hier vorliegt, haben. Es ist zu spät gekommen, das wurde auch schon angesprochen. Es ist zu unausgegoren. Es scheint auch eine große Belastung für Firmen zu sein. Herr Minister, ich weiß ja nicht: Die

Firmen sind auf das Ganze ja nicht wirklich vorbereitet, und wenn schon das Ministerium Schwierigkeiten hat, genügend Experten zu finden, die damit befasst werden, wie sollen das dann private Unternehmungen machen? Das ist der eine Punkt.

Der andere Punkt: Der Experte Lendl hat ausgeführt, dass nicht alle Feedbacks aufgenommen und berücksichtigt werden konnten. – Könnten Sie vielleicht präzisieren, was fehlt oder wer nicht ausreichend gehört oder gewürdigt wurde? Und passend dazu: Wie sehen Sie die Änderungen zum ursprünglichen Ministerialentwurf? Hat sich da etwas verbessert? Hat sich da etwas verschlechtert? Ich bitte also um eine kurze Einschätzung, wie Sie die Änderungen sehen.

Zu Herrn Kneidinger: Sie haben unter anderem auch von datenschutzrechtlichen Bedenken, von überschießenden Befugnissen und Kompetenzen gesprochen. Sie haben, wenn ich das richtig verstanden habe, auch die Gefahr einer möglichen Massenüberwachung gesehen. Können Sie das – die Gefahr der Massenüberwachung – vielleicht ein bisschen vertiefen und ein bisschen näher ausführen, wie das in der Praxis aussehen könnte?

Das waren im Wesentlichen meine Fragen an die Experten. Ich habe mir erlaubt, auch eine an den Minister zu stellen, vielleicht können wir das in der Diskussion ja dann noch erörtern.

Wir Freiheitliche werden aufgrund der massiven Bedenken, die es vor allem im datenschutzrechtlichen Bereich, aber auch hinsichtlich der Bürokratie, der Belastung für private Unternehmungen, die ja bei jedem Betriebsbesuch über die ausufernde Bürokratie klagen, gibt, und aufgrund der Unausgegorenheit und Komplexität, die anscheinend vorliegen, dem, so wie es hier vorliegt, nicht zustimmen.

Abgeordneter Mag. Georg Bürstmayr (Grüne): Danke vielmals an beide Experten für die sehr profunde Einschätzung. Vor diesem Hintergrund und im Interesse eines guten Zeitmanagements gibt es von unserer Seite keine Fragen. –Danke.

Abgeordnete Dr. Stephanie Krisper (NEOS): Ich hätte nur eine Frage, und zwar, ob Sie die Strafbestimmungen weiterhin als überschießend ansehen und ob Ihrer Meinung nach sonst noch Bestimmungen bestehen, die ein Gold Plating darstellen?

Antwortrunde der Experten

Sebastian Kneidinger: Ich probiere, so gut es geht, die gesammelten Fragen zu beantworten, und bitte darum, mich zu erinnern, sollte ich etwas auslassen.

Begonnen hat es, glaube ich, mit der Frage zu den Anforderungen an die Unternehmen. Wir sind sicherlich nicht die Experten, die für die Unternehmen sprechen, daher auch unsere Anregung, die Unternehmen vielleicht noch einmal mit an Bord zu holen. Wir haben, auch bei Konferenzen zu IT-Security und dergleichen, schon mitbekommen, dass noch sehr viel Ungewissheit besteht. Es sind sehr komplexe Anforderungen, es kostet sehr viel Zeit und Geld, das umzusetzen, speziell die Risikomanagementanforderungen. Da muss man bedenken, dass auch stärkere Verantwortlichkeiten für die Geschäftsführung bestehen. Das sind zusätzliche Reportingpflichten, risikomitigierende Maßnahmen – das macht man nicht so schnell.

Unter diesem Gesichtspunkt wäre es auch sehr wünschenswert gewesen, den Entwurf schon viel eher zu haben, denn unserer Erfahrung nach ist es meistens so, dass die Unternehmen den konkreten Entwurf brauchen, um damit umzugehen und sich vorbereiten zu können. Daher sind wir auch in der eigenartigen Situation, dass wir zum einen sagen, dass für die Unternehmen zu wenig Zeit ist, um sich vorzubereiten, gleichzeitig glauben wir aber aufgrund der Ausgestaltung, dass es noch einmal einer Nachbesserung bedarf. Wenn man jetzt den Vergleich zwischen dem Ministerialentwurf und dem Initiativantrag zieht, muss ich sagen: Es hat in gewissen Bereichen ja schon gewisse Besserungen gegeben.

Die nächste Frage würde ich zusammenfassen. Ich glaube, sie betraf die Gefahr der Massenüberwachung, datenschutzrechtliche Bedenken und woraus diese sich konkret ergeben. Dazu würde ich gerne auf die Stellungnahme vom Datenschutzrat

verweisen, die außerordentlich kritisch ist, aber auch auf jene von der Datenschutzbehörde. Ich möchte also hervorheben, dass wir nicht die einzige Organisation sind, die diese Bedenken geäußert hat; ebenso war es auch die Örak. Wenn ich mir das erlauben darf: Das sind alles Institutionen, die nicht dafür bekannt sind, immer mit sehr harten Kritiken oder Stellungnahmen zu kommen, aber so, wie der Entwurf aussieht, war das einfach notwendig.

Zum einen kennt § 17 des NIS-Gesetzes die Möglichkeit zum Betrieb von IKT-Lösungen durch das Bundesministerium für Inneres. Wir halten es jedenfalls für zielführend, dass diese IKT-Lösungen für Unternehmen angeboten werden, denn es besteht auch ein Bedarf dafür. Wir sehen aber die Kritikalität aufgrund der ungenauen Ausgestaltung, aufgrund der ungenauen Textierung und auch, weil es direkt beim Innenministerium ist, weil dort wieder genau jener Zielkonflikt entstehen wird, den wir vorhin aufgezeigt haben. Würden wir den Betrieb der IKT-Lösungen zum Beispiel bei einer nationalen unabhängigen Cybersicherheitsbehörde einrichten und auch ein bisschen nachbessern, welche konkreten Daten verarbeitet werden dürfen, hätten wir viel weniger Bedenken.

Zusätzlich gibt es noch § 42 zur Datenverarbeitung und § 43 zur Datenübermittlung. Da hat es zwischen dem Ministerialentwurf und dem vorliegenden Initiativantrag zwar Nachbesserungen gegeben, konkret wurden die Datenkategorien ergänzt, was natürlich schon einmal ein guter Schritt ist, aber nichtsdestotrotz sind die Zwecke relativ offen. Da haben wir die Problematik, dass halt auch Daten, die eigentlich nur in dem Kontext von ICT-Security verwendet werden sollten, für andere Zwecke verwendet werden. Da gibt es wieder genau das Problem, dass wir davon abhängig sind, dass alle Stakeholder zusammenarbeiten. Wir glauben aber nicht – speziell nach dem Austausch mit den Experten –, dass so eine Gesetzgebung dazu anregt, von selbst mit derlei Informationen an das Innenministerium heranzutreten, das ist das Problem daran.

Die IKT-Lösungen von § 17 bieten natürlich, insbesondere aufgrund der ungenauen Ausgestaltung, relativ viele Möglichkeiten. Insbesondere, wenn es dann um Metadaten, um Überwachung, Sensor Monitoring et cetera geht, gibt es da einfach die Möglichkeit, einen Schritt in Richtung Massenüberwachung zu setzen, vor der wir warnen möchten. Genau deshalb – auch wenn es nicht die Intention des Ministeriums sein mag – glauben wir, dass das Gesetz derart verfasst werden sollte, dass es diese Möglichkeit eben nicht bietet, daher auch unsere Bedenken. Wie gesagt möchte ich aber auch noch einmal auf die Bedenken vom Datenschutzrat dazu verweisen.

Habe ich eine Frage ausgelassen? – Nein, ich glaube, das wäre es dann von meiner Seite.

Mag. Otmar Lendl: Auch ich habe eine lange Liste von Notizen zu dem, was ich jetzt zu beantworten habe.

Punkt eins waren die Maßnahmen: Diese sind für NIS2 noch nicht ganz fix und fertig ausgearbeitet, da ist die Verordnung noch in Ausarbeitung. Wenn Leute zu mir kommen und fragen, was sie erwarten wird, verweise ich meistens auf die Anforderungen aus der NIS1, denn es wird sich nicht viel ändern. Die groben Prinzipien, was Firmen machen müssen, ändern sich nicht dramatisch.

Zur Frage der Kosten: Das ist eine sehr theoretische Frage, denn eigentlich sollte ein guter Kaufmann, ein guter IT-Betrieb, diese Sachen schon gemacht haben. In vielen Bereichen ist das nur die Dokumentation, dass der Stand der Technik hinsichtlich dessen, wie man IT betreiben sollte, auch wirklich erreicht wurde. Wenn man jetzt sagt, man habe dadurch deutlich mehr Aufwände: Ja, die Dokumentation ist die eine Sache, aber die Maßnahmen selber, die technischen Umsetzungen hätten eigentlich eh schon längst passieren sollen.

Zum Thema Zielkonflikte und Co: Ich glaube – was ich aus dem BMI gehört habe –, es gibt dort, auch jetzt mit der neuen Gruppe, dem nationalen Cybersicherheitszentrum, schon eine klare Einteilung in den Bereich Regulierung und in den Bereich

Kooperation. Das heißt, dort ist durchaus das Wissen über diese Konflikte vorhanden, und ich sehe auch in dem, was mir zu dem dortigen organisatorischen Aufbau vorliegt, den klaren Willen, das aufzunehmen und das durch internes Firewalling und Aufgabensplitting zwischen den Bereichen auch gut aufzunehmen.

Auf die Frage, warum wir das alles machen, wenn es nicht so super und perfekt ist, lautet die Antwort immer: Was wäre, wenn nicht? – Auch es nicht zu machen verursacht Kosten und Probleme. Wir arbeiten mit einem sehr alten rechtlichen Rahmen von Finanzierung, Strukturen und Co. Ja, das Neue ist nicht in allen Bereichen so, wie ich es mir gewünscht hätte und wie ich es vom Christkind gerne haben wollen würde, aber nichts zu bekommen hat auch Kosten und Nachteile. Ich glaube, in dem Fall nehme ich lieber das nicht ganz perfekte Gesetz, statt kein Gesetz dafür zu haben.

Zu der Frage, was aus den Stellungnahmen rein kam und was nicht: Ich habe nicht den genauen Überblick, was rein gekommen ist, tut mir leid. Was ich aber weiß, ist, dass einiges von den Sachen, die ich eingeworfen habe, rein kam und in vielen Bereichen haben wir durchaus Verbesserung gesehen. Wir sind quasi von einer Alphaversion der Software zu einer Betaversion hochgestiegen. Ob es schon gut genug für eine Version 1.0 und für einen Release ist, darüber kann man jetzt streiten, aber ja, es wurde im Zuge der Begutachtung deutlich besser.

Die Frage nach der Vorratsdatenspeicherung: Aus meinem Blickwinkel sehe ich da ein klares Nein. Dort geht es um das Mapping der IP-Adresse von Kunden, von Privatnutzern. Hier geht es darum, dass man Sensoren vor Firmen aufbaut, um verdächtigen Netzwerkverkehr zu erkennen. Das hat völlig andere technische Parameter, das ist nicht gleichzusetzen.

Die letzte Frage zum Gold Plating: Ich sehe in dem ganzen Text kein Gold Plating. All das, was für die Firmen irgendwie Aufwand verursacht, ist eins zu eins aus Brüssel übernommen. Nein, in dem Text ist kein Gold Plating. – Danke.

Obmann Dr. Christian Stocker erteilt, da auch Fragen an den Herrn Bundesminister gestellt worden sind, diesem nun zu einer kurzen Beantwortung das Wort.

Schlussstatement des Bundesministers

Bundesminister für Inneres Mag. Gerhard Karner: Es ist weniger eine Beantwortung, da zum Teil ja schon sehr detaillierte Fragen dabei waren, zu denen auch die Experten aus unserem Haus einige Sätze sagen werden. Mir geht es nur um ein paar grundsätzlich Punkte, die zu sagen mir in Anwesenheit der Experten auch wichtig ist: Ich bedanke mich für Ihre Expertise, die Sie hier eingebracht und vorgebracht haben. Mir ist nur eines ganz wichtig: Was die ansatzlose Massenüberwachung angeht, so ist klar der Auftrag, sie in diesem Gesetz nicht vorzusehen. Das ist klar der politische Wille und das ist auch mein Auftrag, um das an dieser Stelle noch einmal ganz klar und deutlich zu sagen.

Die zweite Bitte, die ich habe, Herr Kneidinger: Unsere Experten aus dem Haus, gemeinsam mit vielen anderen aus vielen Ressorts, haben intensiv daran gearbeitet, ja, waren auf Touren unterwegs, denn es ist auch politische Arbeit, Touren zu machen. Dort hinten sitzt beispielsweise Philipp Blauensteiner, der intensiv mit vielen Unternehmer:innen, großen Unternehmen, Klein- und Mittelbetrieben gesprochen hat, sie sensibilisiert hat, darauf vorbereitet hat, was da auf uns – auf uns – zukommen wird. Wie schwierig dieser Schritt ist, unterstreicht diese Diskussion.

Daher nur als letzten Satz – das muss und will ich sagen, es ist mir ein Anliegen – : Unseren Mitarbeiterinnen und Mitarbeitern mangelnde Ernsthaftigkeit nachzusagen – das haben Sie in Ihrer Anfangsstellungnahme leider getan –, ist etwas, was ich gegenüber unseren Mitarbeiterinnen und Mitarbeitern so nicht stehen lassen kann. Inhaltliche Kritik ja, aber mangelnde Ernsthaftigkeit nein.

Obmann Dr. Christian Stocker erklärt das Hearing und damit den öffentlichen Teil der Sitzung für ***beendet.***

Auszugsweise Darstellung

Ausschuss für innere Angelegenheiten – XXVII. GP 19. Juni 2024 28. Sitzung / 23

Schluss des öffentlichen Teils von TOP 1: 13.48 Uhr

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2025-03-28T19:35:48+01:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	