An das
Bundesministerium für Wissenschaft,
Forschung und Wirtschaft
z.H. Mag.iur. Katharina Kühmayer
RECHTSABTEILUNG – AUSSENWIRTSCHAFT (C2/1)
Stubenring 1
1011 Wien

E-Mail: not9834@bmwfw.gv.at

Wien, am 20. Februar 2015

BETREFF: ISPA-STELLUNGNAHME ZUM DEUTSCHEN ENTWURF EINES GESETZES ZUR EHÖHUNG DER SICHERHEIT INFORMATIONSTECHNISCHER SYSTEME – IT-SICHERHEITSGESETZ, NOTIFIKATION NR.: 2014/635/D

Sehr geehrte Damen und Herren,

die ISPA erlaubt sich im Zusammenhang mit der öffentlichen Konsultation des Bundesministeriums für Wissenschaft, Forschung und Wirtschaft im Rahmen des EG-Infoverfahrens betreffend den deutschen Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), Notifikation Nr. 2014/635/D nachstehende Anregungen zu liefern.

Die ISPA verweist darauf, dass sich unter ihren rund 200 Mitgliedern zahlreiche Unternehmen befinden, die sowohl in Deutschland als auch in Österreich aktiv sind. Der zu konsultierende Gesetzesvorschlag könnte zu stark divergierenden IT-Sicherheitsstandards für die Kommunikationsinfrastruktur in der EU führen und somit die europäischen Harmonisierungsbestrebungen in diesem Bereich hemmen. Die Durchsetzung von europaweiten einheitlichen Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit ist das Hauptziel des Vorschlages der NIS-Richtlinie und stellt eine unabdingbare Voraussetzung für die Vollendung des digitalen Binnenmarkts sowie für das reibungslose Funktionieren des Binnenmarkts überhaupt dar.

Die ISPA hebt hervor, dass ein Einklang zwischen nationalen Gesetzesentwürfen und der NIS-Richtlinie sicherzustellen ist und steht nationalen Alleingängen in diesem Bereich abweisend gegenüber. ISPA begrüßt die Ausnahme von Anbietern öffentlicher Kommunikationsnetze und -dienste sowie von Kleinstunternehmen aus dem Anwendungsbereich des BSI-Gesetzes n.F. und der damit verbundenen Verhinderung sowie Beseitigung von Doppelregulierungen (z.B. Meldepflichten für ein und denselben Vorfall aufgrund unterschiedlicher rechtlicher Vorgaben an unterschiedliche Stellen). ISPA gibt zudem zu bedenken, dass das Herabsenken der Schwelle für eine Meldepflicht auf die Möglichkeit einer „beträchtlichen Beeinträchtigung“ unter Umständen zu weitgehend ist und der Adressatenkreis der Bestimmung im Telemediengesetz, der sämtliche

Dienste der Informationsgesellschaft und so unter Umständen auch Blogs oder einzelne Social-Media-Plattformen betrifft, zu umfangreich ist. Abschließend möchte die die ISPA darauf hinweisen, dass die Informationspflicht gem. § 109a dtTKG für die Betreiber einen erheblichen organisatorischen Aufwand bedeuten würde, der in Relation zu dem zu erwartenden Nutzen kritisch zu hinterfragen ist.

1. **Die Konformität mit der NIS-Richtlinie ist sicherzustellen und nationale Alleingänge sind abzulehnen.**

Bei IT-Sicherheit handelt es sich im Zeitalter globaler Vernetzung um eine typischerweise grenzüberschreitende Angelegenheit, deshalb setzen wirksame Verbesserungen der IT-Sicherheit von Kommunikationsinfrastruktur europaweit abgestimmte Bestimmungen und Standards voraus, die über Staatsgrenzen hinaus wirkende Sicherheitsmaßnahmen und Regelungen durchsetzen können.

Vor dem Hintergrund des aktuellen europäischen Gesetzgebungsverfahrens für eine Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit („NIS-Richtlinie“), welche bereits 2015 abgeschlossen werden soll, wäre es begrüßenswert, wenn die Bestimmungen eines nationalen Gesetzesentwurfs den inhaltlichen Gleichklang mit den Bestimmungen der NIS-Richtlinie wahrten.

Auf dem Weg zu einem gemeinsamen europäischen digitalen Binnenmarkt würden sich nationale Alleingänge in diesem Bereich als problematisch darstellen. Darüber hinaus erscheint eine Abgleichung der datenschutzrechtlich relevanten Bestimmungen des Entwurfes mit den zukünftig europaweit geltenden Bestimmungen der Datenschutz-Grundverordnung als ein überaus sinnvoller Schritt.

2. **Die Einschränkung des Anwendungsbereich des BSI-Gesetzes n.F ist zu begrüßen.**

Die ausdrückliche Ausnahme der Anbieter von öffentlichen Kommunikationsnetzen und –diensten und Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG aus dem Regelungsbereich des Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes (BSI-Gesetz) ist zu begrüßen. Die damit verbundene Beseitigung von Doppelregulierungen (z.B. Meldepflichten für ein und denselben Vorfall aufgrund unterschiedlicher rechtlicher Vorgaben an unterschiedliche Stellen) sowie die Anlehnung an den Adressatenkreis der NIS-Richtlinie erscheinen jedenfalls begrüßenswert.

3. **Das Herabsenken der Schwelle für eine Meldepflicht auf die „Möglichkeit einer beträchtlichen Beeinträchtigung“ ist sehr weitgehend und daher zu hinterfragen.**

Die Meldeschwelle für bereits jetzt bestehende Meldepflicht für Anbieter von Telekommunikationsnetzen- und -diensten soll gemäß § 109 Abs.5 dtTKG erheblich abgesenkt werden. Statt wie bisher tatsächliche Sicherheitsverletzungen, wären hinkünftig sämtliche Beeinträchtigungen, die die „Möglichkeit“ einer beträchtlichen Sicherheitsverletzung mit sich brächten, zu melden.

Das Herabsenken der Schwelle für eine Meldepflicht auf die Möglichkeit einer beträchtlichen Beeinträchtigung wäre wohl zu weitgehend. Dies gilt insbesondere in Hinblick auf den strengeren Tatbestand der „bedeutenden Störung“ gemäß § 8b Abs 4 BIS-Gesetz, der für sonstige Betreiber kritischer Infrastruktur zur Anwendung kommt.

Die im Entwurf vorgesehene Meldeschwelle erscheint zudem ausgesprochen unbestimmt. Wann genau ein meldepflichtiges Ereignis vorliegt, wäre für die Unternehmen aus der Definition nicht ablesbar. Auch im Sinne der Wirtschaftlichkeit wäre es den Behörden wohl nur schwer zuzumuten, jede Meldung über auch noch so einen unbedeutenden Vorfall prüfen zu müssen. Aus Sicht der Telekommunikationsunternehmen ist zudem auch nicht nachvollziehbar, warum sonstige Betreiber kritischer Infrastrukturen die Möglichkeit der anonymen Meldung erhalten, während Unternehmen, die aufgrund der Bestimmungen des dtTKG melden, diese Möglichkeit nicht eingeräumt wird. Diesbezüglich erscheint eine Vereinheitlichung erstrebenswert.

4. **Die Informationspflicht gem. § 109a dtTKG würde für die Betreiber einen erheblichen organisatorischen Aufwand mit sich bringen und ist im Lichte ihres potenziellen Nutzens kritisch zu hinterfragen.**

Die Neuregelung des § 109a dtTKG sieht vor, dass Anbieter, sofern ihnen Störungen bekannt werden, die von Datenverarbeitungssystemen der Nutzerinnen und Nutzer ausgehen, diese darüber informieren müssen. Diese Information soll die Nutzerinnen und Nutzer in die Lage versetzen, selbst Maßnahmen gegen die auf ihren Systemen vorhandene Schadsoftware zu ergreifen. Ergänzend zur Informationspflicht würden Anbieter von öffentlichen Telekommunikationsdiensten verpflichtet, soweit es technisch möglich und zumutbar ist, die Nutzerinnen und Nutzer auf einfach bedienbare Sicherheitswerkzeuge hinzuweisen, die sowohl vorbeugend als auch zur Beseitigung von Störungen bei einer bereits erfolgten Infizierung des Datenverarbeitungssystems mit Schadsoftware eingesetzt werden können.

Vorweg ist anzumerken dass die ISPA den Gedanken des „Empowerment“ von Nutzerinnen und Nutzern unterstützt. Die Anbieter bieten daher von sich aus bereits jetzt Informationen über die Vermeidung von Sicherheitsherausforderungen an. Die ISPA regt deshalb an, den Bedarf für eine derartige Vorschreibung von Informationspflichten vorweg zu evaluieren. Sofern tatsächlich einen solchen Bedarf festgestellt wird, soll dieser im Rahmen des Connecting European Facilities (CEF) Förderprogrammes der EU gedeckt werden bzw. sollen Förderungen für in den Mitgliedstaaten bereits laufende Safer Internet Projekte erhöht werden.

Diese Informationspflichten bergen für Betreiber von Telekommunikationsdiensten einen erheblichen organisatorischen Aufwand und sind angesichts des Adressatenkreises völlig uferlos und praxisfern. Daher sollten diese auch im Hinblick auf den potentiellen Nutzen sowie die bereits existierenden Maßnahmen neu überdacht werden.

5. Der Adressatenkreis der Bestimmungen im Telemediengesetz ist zu umfangreich.

Die Verbesserung von IT-Mindestsicherheitsstandards für Dienste der Informationsgesellschaft (deutscher Begriff „Telemediendienste“) ist ein begrüßenswerter Ansatz, in Hinblick auf den weiten Adressatenkreis ist die Bestimmung des § 13 Abs. 7 TMG n.F. jedoch zu umfangreich.

Nach der aktuellen Definition wären sämtliche Dienste der Informationsgesellschaft umfasst, die gewerblich, also in der Regel gegen Entgelt, angeboten werden. Diese Definition wird äußerst weit ausgelegt und betrifft unter Umständen auch Blogs oder einzelne Social-Media-Accounts. Ein beträchtlicher Teil der durch diese Definition betroffenen Anbieter wären weder technisch noch organisatorisch in der Lage, die gesetzlich geforderten Verpflichtungen umzusetzen.

Eine Eingrenzung der Sicherstellungsverpflichtung auf „soweit technisch möglich und zumutbar“ erscheint der ISPA daher zu kurz gegriffen.

Die ISPA hoffte auf die Aufnahme und Weitergabe ihrer Bedenken und Anregungen.

Für Rückfragen (und weitere Auskünfte) stehen wir jederzeit gerne zur Verfügung.

Mit freundlichen Grüßen,

ISPA - Internet Service Providers Austria

Dr. Maximilian Schubert

Generalsekretär

Die ISPA – Internet Service Providers Austria –ist der Dachverband der österreichischen Internet Service-Anbieter und wurde im Jahr 1997 als eingetragener Verein gegründet. Ziel des Verbandes ist die Förderung des Internets in Österreich und die Unterstützung der Anliegen und Interessen von rund 200 Mitgliedern gegenüber Regierung, Behörden und anderen Institutionen, Verbänden und Gremien. Die ISPA vertritt Mitglieder aus Bereichen wie Access, Content und Services und fördert die Kommunikation der Marktteilnehmerinnen und Marktteilnehmer untereinander.