IT-Sicherheit-Gesetzgebung aus europäischer Perspektive

Oliver Süme
(Vorstand Politik & Recht eco – Verband der deutschen Internetwirtschaft)

WIR GESTALTEN DAS INTERNET.

Verband der deutschen Internetwirtschaft e.V.

Europa: **„NIS-Richtlinie“ (Network- and Information Security)**

- **Ziel:** Harmonierung der gesetzlichen Verpflichtungen zur IT-Sicherheit auf europäischer Ebene (Mindestharmonisierung, RL muss von den Mitgliedsstaaten in nationales Recht umgesetzt werden)

- Richtlinien-Vorschlag ist Teil der Strategie für einen Europäischen Digitalen Binnenmarkt

„NIS-Richtlinie“ (Network- and Information Security)

Zentrale Regelungen:

- Alle Mitgliedstaaten müssen
  - nationale NIS-Strategien entwickeln,
  - ein Mindestniveau nationaler Kapazitäten im Bereich der Netz- und Informationssicherheit zu schaffen, eine für NIS zuständige Behörden einrichten, die angemessenen, personell, finanziell und technisch ausgestattet ist.

„NIS-Richtlinie“

- **IT-Notfallteams** (Computer Emergency Response Teams – CERT) einzurichten,
- ein gemeinsames Kooperationsnetz zur Bewältigung von Sicherheitsrisiken und Vorfällen zu bilden.
- Die Europäische Agentur für Netz- und Informationssicherheit (ENISA) soll die Arbeit dieses Netzes auf Anfrage unterstützen,

„NIS-Richtlinie“

- **Mindeststandards:** Unternehmen sollen verpflichtet werden, die Risiken, denen sie unterliegen, zu bewerten und geeignete und angemessene Maßnahmen zur Gewährleistung der NIS zu ergreifen.

- **Meldepflicht:** Den zuständigen Behörden müssen alle Sicherheitsvorfälle gemeldet werden, welche ihre Netze und Informationssysteme wie auch die Kontinuität kritischer Dienste beeinträchtigen.

„NIS-Richtlinie“

Zeitplan:

7.2.2013: COM stellt Vorschlag für eine RL vor

13.03.2014: EP beschließt Vorschlag mit Änderungen

seit Oktober 2014: informeller Trilog, noch keine Einigung; Verhandlungen kommen langsam voran

Mai 2015: Vorstellung der Strategie für einen Digitalen Binnenmarkt in Europa

Ausblick:

seit September 2015:

weitere Trilog-Verhandlungen, umstritten ist insb. der Anwendungsbereich (Wer soll von der Richtlinie betroffen sein?)

Dezember 2015:

Angestrebter Einigungsbeschluss des Ministerrats

Ausblick:

Die Richtlinie soll 20 Tage nach Verabschiedung und Veröffentlichung in Kraft treten.

Nach derzeitigem Verhandlungsstand beträgt die Umsetzungsfrist für die Mitgliedsstaaten **1 Jahr und 6 Monate** .

Die Mitgliedstaaten müssten die RL dann spätestens **bis Mitte 2016** in nationales Recht umgesetzt haben.

„NIS-Richtlinie“

Offene Fragen im Rahmen des Gesetzgebungsverfahrens:

1. Wieviel Spielraum soll den Mitgliedstaaten bei der Identifikation kritischer Infrastrukturen eingeräumt werden?

2. Inwieweit sollten „internet enabler“ bzw. Dienste der Informationsgesellschaft einbezogen werden?

eco Positionen zur „NIS-Richtlinie“:

- Harmonisierende Regulierung im Bereich der IT-Sicherheit kritischer Infrastrukturen notwendig und begrüßenswert

eco Positionen zur „NIS-Richtlinie“:

- Fragmentierung und Umsetzungsunterschiede verhindern

eco Positionen zur „NIS-Richtlinie“:

- Konzentration des Anwendungsbereichs auf tatsächlich kritische Infrastrukturen

eco Positionen zur „NIS-Richtlinie“:

- Keine Sonderregelungen für sämtliche Dienste der Informationsgesellschaft, sondern ein am jeweiligen Ausfallrisiko orientierter Ansatz

eco Positionen zur „NIS-Richtlinie“:

- Berücksichtigung bereits bestehender branchenspezifischer Verpflichtungen aufrechterhalten

Vielen Dank!

Verband der deutschen Internetwirtschaft e.V.

WIR GESTALTEN DAS INTERNET.

eco

weitere Fragen:

Wo sollte aus Sicht der Internetwirtschaft der Fokus des europäischen Gesetzgebers liegen?

weitere Fragen:

Ist die Abstimmung mit bereits existierenden nationalen Regelungen, z.B. dem deutschen IT-Sicherheitsgesetz, gewährleistet?

weitere Fragen:

Welche Problematiken berührt die Richtlinie gar nicht?