Netzsicherheit

Die NIS-Richtlinie und ihr Beitrag zur Netzsicherheit

Bundeskanzleramt/Präsidium
Abt. I/11 – Digitales und E-Government – Recht, Strategie und Internationales

gregor.schmied@bka.gv.at

Hintergründe

- Netz- und Informationssysteme spielen eine zentrale gesellschaftliche Rolle in Europa und müssen **verlässlich und sicher** sein.
- Sicherheitsvorfälle, insb. Cyber-Angriffe nehmen stetig zu **(Quantität + Qualität)**
- Folgen:
  - Beeinträchtigung wirtschaftlicher Tätigkeiten
  - Beträchtliche finanzielle Verluste möglich
  - Vertrauensverlust bei den Nutzern
  - Großer wirtschaftlicher Schaden für die Union
- Derzeit bestehen unterschiedliche Niveaus der Abwehrbereitschaft in den MS → umfassender und **einheitlicher Ansatz auf Unionsebene** ist erforderlich

Österreich:
Bericht Cyber Sicherheit 2016

- Jährlicher Bericht im Rahmen der ÖSCS
- Zusammenfassende Darstellung der Cyber Bedrohungen und wesentlicher nationaler und internationaler Entwicklungen

Download unter:
https://www.bka.gv.at/DocView.axd?CobId=63191

Ziel: EU-weit ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen zu gewährleisten

- **(1) Stärkung der Zusammenarbeit** zwischen den MS
- **(2)** Verpflichtung zur Einführung angemessener **IT-Sicherheitsmaßnahmen** und der **(2)** Verpflichtung zur **Meldung signifikanter Störfälle** für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste

Verpflichtungen für MS

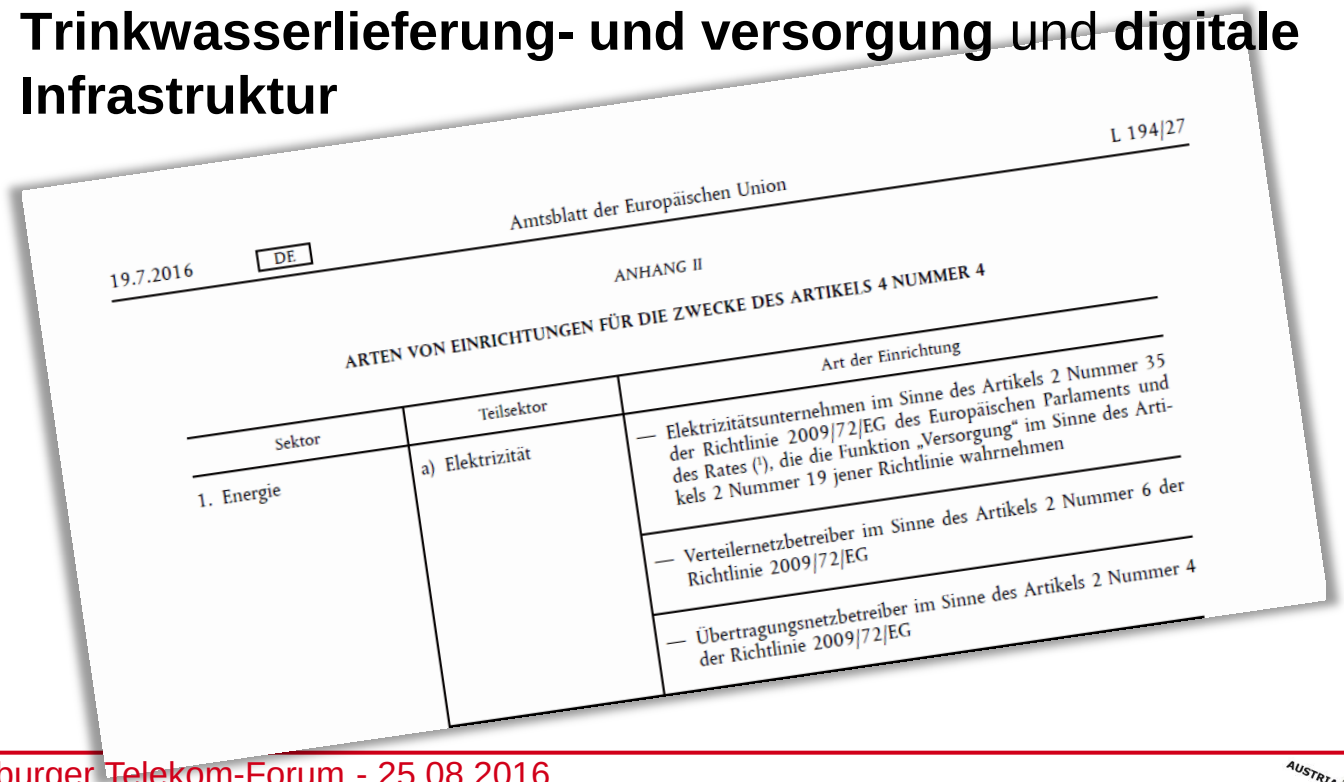
- Annahme einer **nationalen Strategie für die Sicherheit von Netz- und Informationssystemen**
- Bildung nationaler **CSIRTs**
- Einrichtung einer/mehrerer **NIS-Behörde(n) und** eines **SPOCs**
- Teilnahme an der **strategischen Kooperationsgruppe** und des **operativen CSIRT-Netzwerks**
- **Ermittlung** von Betreibern wesentlicher Dienste
- Möglichkeit für **freiwillige Meldungen** schaffen
- **Sanktionen** festlegen

Computer-Notfallteams (CSIRTs)

- **C**omputer **S**ecurity **I**ncident **R**esponse **T**eams
  - Auch CERTs (Computer Emergency Response Teams) genannt
- techn. Unterstützung für betroffene Einrichtungen bei der Bewältigung von Sicherheitsvorfällen
- Anforderungen:
  - hoher Grad der Verfügbarkeit ihrer Kommunikationsnetze
  - an sicheren Standorten eingerichtet
  - ständige Bereitschaft (personell)
  - Verfügbarkeit der Infrastruktur muss sichergestellt sein (Redundanzsysteme, Ausweicharbeitsräume)

Anwendungsbereich (1)

- **Betreiber wesentlicher Dienste:**
  - **Öffentliche** oder **private** Einrichtung
  - aus den Sektoren **Energie, Verkehr,Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserlieferung- und versorgung** und **digitale Infrastruktur**



19.7.2016 DE Amtsblatt der Europäischen Union L 194/27

ANHANG II

ARTEN VON EINRICHTUNGEN FÜR DIE ZWECKE DES ARTIKELS 4 NUMMER 4

Sektor	Teilsektor	Art der Einrichtung
1. Energie	a) Elektrizität	— Elektrizitätsunternehmen im Sinne des Artikels 2 Nummer 35 der Richtlinie 2009/72/EG des Europäischen Parlaments und des Rates (1), die die Funktion „Versorgung" im Sinne des Artikels 2 Nummer 19 jener Richtlinie wahrnehmen
		— Verteilernetzbetreiber im Sinne des Artikels 2 Nummer 6 der Richtlinie 2009/72/EG
		— Übertragungsnetzbetreiber im Sinne des Artikels 2 Nummer 4 der Richtlinie 2009/72/EG

Kriterien zur Ermittlung von Betreibern wesentlicher Dienste

- **Niederlassung** im Hoheitsgebiet des MS
- Einrichtung betreibt **Dienst**, der für die Aufrechterhaltung **kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten** unerlässlich ist
- Bereitstellung dieses Dienstes ist **abhängig von Netz- und Informationssystemen**
- Sicherheitsvorfall würde **erhebliche Störung bei der Bereitstellung** dieses Dienstes bewirken

Erhebliche Störung (Art. 6)

- **Sektorübergreifende Faktoren:**
  - Zahl der Nutzer
  - Abhängigkeit anderer Sektoren aus Anhang II
  - Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten oder die öffentliche Sicherheit
  - Marktanteil des Betreibers
  - Geografische Ausbreitung des Gebiets, das von dem Sicherheitsvorfall betroffen sein könnte
  - Verfügbarkeit von alternativen Mitteln für die Bereitstellung des Dienstes
- **MS haben auch sektorspezifische Faktoren zu beachten**

Ausnahmen

- Unternehmen, die den Anforderungen der Art. 13a und 13b Rahmenrichtlinie unterliegen
- **Vertrauensdiensteanbieter**, die den Anforderungen des Art. 19 eIDAS-VO unterliegen
- Andere **einschlägige sektorspezifische Rechtsakte** der Union gehen ebenfalls der NIS-RL vor

Anwendungsbereich (2)

- **Anbieter digitaler Dienste**
  - **Juristische** Person
  - Bietet einen der drei in der RL genannten **digitalen Dienste** an
    - Online **Marktplatz**
    - Online **Suchmaschine**
    - **Cloud**-Computing-Dienst
  - **Ausnahmen:**
    - natürliche Personen
    - Klein- und Kleinstunternehmen
  - **Keine Ermittlung** durch MS!
    - RL soll im Rahmen ihres Geltungsbereiches für alle Anbieter digitaler Dienste gelten

Verpflichtung für Betreiber und Anbieter

- **(1)** Pflicht angemessene technische und organisatorische **Sicherheitsmaßnahmen** zur **Risikobewältigung** zu ergreifen
  - Stand der Technik; Angemessenheit
  - Anwendung international anerkannter Normen und Spezifikationen für die Sicherheit von Netz- und Informationssystemen
- **(2)** Pflicht zur **unverzüglichen Meldung von Störfällen,** die **erhebliche** Auswirkungen (betroffene Nutzer, Dauer, geografische Ausbreitung) auf die **Verfügbarkeit** der bereitgestellten wesentlichen Dienste haben
  - Meldung ergeht an **NIS-Behörde** oder an **CSIRTs**

Unterscheidung Betreiber und Anbieter

- **Strengere nationale Regelungen** nur für Betreiber wesentlicher Dienste möglich
  - EK erlässt **Durchführungs-RA** zu den **Sicherheitsanforderungen** und **Meldepflichten** für Anbieter digitaler Dienste
  - **Ziel:** hohes Maß an **Harmonisierung** in Bezug auf Anbieter digitaler Dienste
- **Prüfung der Sicherheitsmaßnahmen** durch NIS-Behörde:
  - **Betreiber** → jederzeit → Ergebnis: bindende Anweisungen
  - **Anbieter digitaler Dienste** → konkreter Anlassfall → Ergebnis: Fehlerbehebung einfordern
- **Zuständigkeit**:
  - **Betreiber**: MS in dem der Betreiber eine **Niederlassung** hat (können auch mehrere MS sein)
  - **Anbieter digitaler Dienste: MS der Hauptniederlassung** (nur dieser); Pflicht zur Namhaftmachung eines **Bevollmächtigten** wenn keine EU-Niederlassung

„NIS-Behörde(n)“- Aufgaben:

- **Überwachen** die Anwendung der RL auf nationaler Ebene
- **Prüfung der Sicherheitsmaßnahmen**
  - Von Betreibern wesentlicher Dienste (jederzeit)
  - Von Anbietern digitaler Dienste (ex post)
- **Meldestelle** von Störfällen (auch CSIRT)
- Bestimmung möglicher **grenzüberschreitende Auswirkungen** und Kontaktaufnahme zu den betroffenen MS (auch CSIRT)
- **Information der Öffentlichkeit über individuelle Vorfälle** wenn im öffentlichen Interesse gelegen (auch CSIRT)

CSIRTs und SPOC - Aufgaben

- ein oder mehrere **CSIRTs:**
  - Kontinuierliche **Risikoanalyse** und **Situationsbewusstsein**
  - Ausgabe von **Frühwarnungen**, **Verbreitung von Informationen** über Risiken und Vorfälle
  - Monitoring und Handling von **Störfällen**
  - **Meldestelle** von Störfällen (auch NIS-Behörde)
  - Bestimmung über **grenzüberschreitendes Potential eines Störfalls** (auch NIS-Behörde)
  - Teilnahme am **CSIRT-Netzwerk** auf EU-Ebene

- **Single Point of Contact (SPOC):**
  - **Verbindungsstelle** zwischen **MS, Kooperationsgruppe und CSIRT-Netzwerk**

Kooperationsgruppe - strategische Aufgaben

- **Teilnehmer**: Vertreter aus **MS**, **EK** und **ENISA**
- **Beginn** der Tätigkeit: bis spätestens **Februar 2017**
- **Aufgaben u.a.**:
  - Strategische Beratung des **CSIRT-Netzwerks**
  - Erstellung von **Leitlinien** für sektorspezifische **Kriterien** zur Bestimmung der **„Signifikanz“ eines Vorfalls**
  - **Unterstützung in der Identifikationsphase** der Betreiber – MS sollen einen kohärenten Ansatz finden (Art. 24 Abs. 2)
  - Austausch von **Informationen** und **bester Praktiken**
    - **Meldung von** Störfällen
    - **Identifikation** von Betreibern
    - **Bewusstseinsbildende** Maßnahmen
    - **Forschung und Entwicklung** im NIS-Bereich

CSIRT-Netzwerk - operative Aufgaben

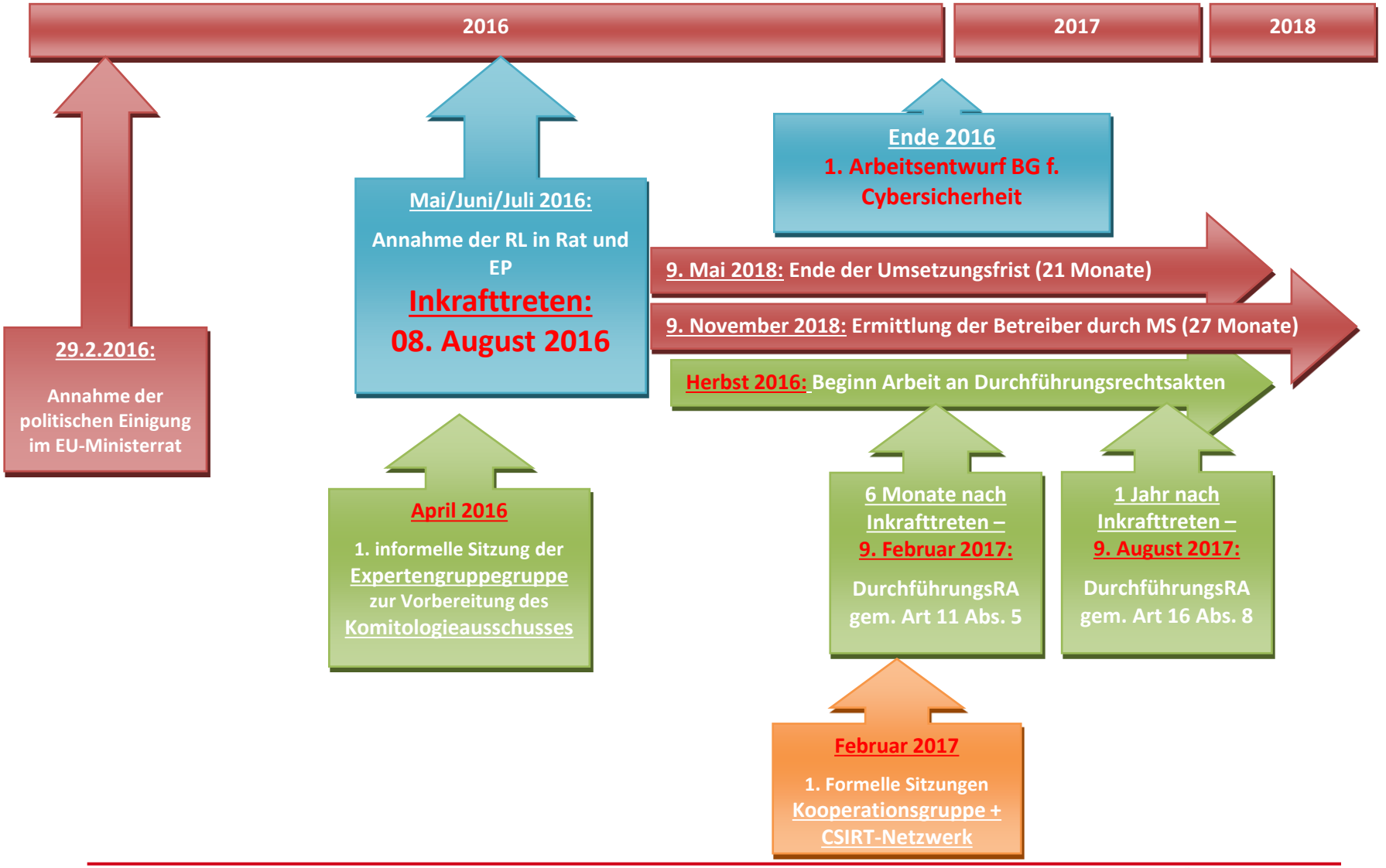
- **Teilnehmer**: Vertreter der **nat. CSIRTs** und **CERT-EU** (EK hat Beobachterrolle)
- **Aufgaben u.a.:**
  - **Vertrauensaufbau** zwischen den MS
  - **Allgemeiner Informationsaustausch** über **Störfälle**
  - **Assistenz** bei **länderübergreifenden Vorfällen**
  - Auf Ersuchen eines MS: **koordinierte Reaktion** auf einen Störfall der sich im Zuständigkeitsbereich des ersuchenden MS ereignet hat
  - **Erfahrungsaustausch** nach **NIS-Übungen**

Durchführungsrechtsakte

- **Kooperationsgruppe**
  - Art. 11 Abs. 5: Verfahrensmodalitäten festlegen
    - Erster Entwurf bis 9. Februar 2017

- **Digitale Diensteanbieter**
  - Art. 16 Abs. 8: Konkretisierung der Sicherheitsmaßnahmen und Erheblichkeit eines Sicherheitsvorfalls
    - Zu erlassen bis 9. August 2017
  - Art. 16 Abs. 9: Form und Verfahren für Meldepflicht
    - Keine Frist; Optional

Zeitplan NIS-RL:



Umsetzung in Österreich

ÖST. CYBER-SICHERHEITSGESETZ

Arbeitsprogramm der Bundesregierung

- 2013-2018
- Schutz kritischer Infrastrukturen und **Erhöhung der Sicherheit des „Cyber-Raums“** und der Menschen im „Cyber Space“ im Zusammenwirken von Staat, Wirtschaft, Wissenschaft und Gesellschaft
- **„Österreichische Strategie für Cyber-Sicherheit“ (ÖSCS)**
- Koordination auf operativer Ebene im Bereich „Cyber-Sicherheit“
- Verhandlungen zur NIS-RL auf EU-Ebene
- Schaffung eines **Bundesgesetzes zur „Cyber-Sicherheit“**

ÖSCS - AG Ordnungspolitischer Rahmen

- Parallel zu Verhandlungen der NIS-RL
- Interministerielle Zusammensetzung
- Ziel: den **bestehenden ordnungspolitischen Rahmen** sowie darauf aufbauend notwendige Änderungen zu untersuchen
- Übergang in eine interministerielle AG zur Erarbeitung eines BG für Cybersicherheit (Kick-Off Februar 2016)
  - ➢ **Querschnittsmaterie!**

Umsetzungsoptionen zur NIS-RL

- **(1) Behörden:**
  - Drei zuständige Behörden in Österreich
  - Aufgabenaufteilung nach **strategischen** und **operativen** Gesichtspunkten
  - Bereits bestehende Strukturen/Organisationen nutzen

- **(2) Meldefluss und freiwillige Meldung:**
  - Verpflichtete und freiwillige Meldungen gehen an die **CSIRTs**
  - CSIRTs geben diese unverzüglich an Behörden weiter
  - Freiwillige Meldungen nur in **anonym**isierter Form

Umsetzungsoptionen zur NIS-RL

- **(3) Einbeziehung anderer Sektoren**
  - **Öffentlicher** Bereich
  - **Telekommunikationssektor** ist vom Anwendungsbereich der RL explizit ausgenommen
  - Ebenso: **Vertrauensdiensteanbieter** nach eIDAS-VO
  - Bestehen sektorspezifische Rechtsakte mit gleichwertigen Verpflichtungen für Betreiber oder digitale Diensteanbieter, so gehen diese der NIS-RL vor

➢ **Ziel:** Parallel bestehende Meldepflichten zusammenführen und Synergien erzeugen

Regelungsnotwendigkeiten

- Organisation der **Cybersicherheits-Struktur(en) in Ö**
- **Informationsaustausch + Informationsgewinnung**
  - Zwischen Privaten
  - Zwischen Behörden
  - zwischen Behörden und Privaten
- Melde**verpflichtung** und Melde**recht (freiwillige Meldungen)**
- Verpflichtende **Sicherheitsmaßnahmen** und **IT-Risikomanagement**
- **Sanktionen** (Strafmaß? - vgl. EU-DSGV)

Danke für Ihre Aufmerksamkeit!

Fragen?

Bundeskanzleramt Österreich/Präsidium
Abt. I/11: Digitales und E-Government - Recht, Strategie und Internationales

Mag. Gregor Schmied

Ballhausplatz 1, 1014 Wien
Tel.: +43 1 531 15-202591
E-Mail: gregor.schmied@bka.gv.at