NIS-RL und die Umsetzung im NISG

17.12.2018
Datenschutz “neu”:
Erste Erfahrungen und neue Herausforderungen

Mag. Verena Becker, BSc
Bundessparte Information und Consulting

WIR
SCHAUEN AUF ÖSTERREICH
WKO
WIRTSCHAFTSKAMMER ÖSTERREICH

Inhalt

- Zeitablauf
- NIS-RL
  - Allgemeines
  - Inhalt
  - Betroffene
- NISG
  - Behörden
  - Verpflichtungen
  - Sanktionen

Timeline

- 7. Februar 2013:
  - Mitteilung zur "Cybersicherheitsstrategie der Europäischen Union“
  - Vorschlag für eine Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit (NIS-RL)
- 8.8.2016: Inkrafttreten NIS-RL (2016/1148)
- 9.5.2018: Ende Frist für die nationale Umsetzung
- 10.5.2018: DfV(EU)2018/151 betreffend Anbieter digitaler Dienste
- 11.12.2018: NISG im Nationalrat
- 19.12.2018: NISG im Bundesrat
- bis Mitte Jänner 2019: Inkrafttreten NISG
- Ende Jänner-Mitte Februar: VO zu § 16 Abs. 2 (Regelungen für Sektoren)
- Februar-April 2019: Ermittlung Betreiber wesentlicher Dienste (Bescheid)

NIS-Richtlinie - Allgemeines

- Richtlinie 2016/1148 über Maßnahmen zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen in der Union
- erste EU-weite Regelung zu Cybersicherheit
- Verlässlichkeit von Netz- und Informationssystemen entscheidend für Wirtschaft, Gesellschaft und Binnenmarkt
- Ziel: hohes Sicherheitsniveau der Netz- und Informationssicherheitssysteme
- Mindestharmonisierung

NIS-Richtlinie - Inhalt

- einheitlicher Rechtsrahmen für den EU-weiten Aufbau nationaler Kapazitäten für Cyber-Sicherheit
- Zusammenarbeit der Mitgliedstaaten
- nationale NIS-Strategien
- Mindestanforderungen Sicherheitsvorkehrungen und Meldepflichten für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste
- Sanktionen: „wirksam, angemessen und abschreckend“

NIS-Richtlinie - Anwendungsbereich

- Betreiber wesentlicher Dienste
- Anbieter digitaler Dienste
- NICHT: öffentliche Verwaltung (national möglich)

NIS-RL - Betreiber wesentlicher Dienste

- öffentliche oder private Einrichtung
- Sektoren:
  - Energie
  - Verkehr
  - Bankwesen,
  - Finanzmarktinfrastrukturen
  - Gesundheitswesen
  - Trinkwasserlieferung und -versorgung
  - digitale Infrastruktur
- Niederlassung im Hoheitsgebiet des MS
- Dienst für die Aufrechterhaltung kritischer gesellschaftlicher und/oder wirtschaftlicher Tätigkeiten unerlässlich
- abhängig von Netz-und Informationssystemen
- Sicherheitsvorfall → erhebliche Störung bei der Bereitstellung dieses Dienstes
- unabh. von Größe

NIS-Richtlinie - Anbieter digitaler Dienste

- Juristische Person:
  - Online Marktplatz
  - Online Suchmaschine
  - Cloud Computing-Dienst
- Ausnahmen:
  - Kleinunternehmen:
    < 50 Mitarbeiter UND Jahresumsatz/bilanz < 10 Mio. EUR
  - Kleinstunternehmen:
    < 10 Mitarbeiter UND Jahresumsatz/bilanz < 2 Mio. EUR
- Vollharmonisierung:
  - keine **Ermittlung** durch MS!
  - Durchführungsverordnung (EU) 2018/151 vom 30. Januar 2018: Sicherheitselemente, Sicherheitsvorkehrungen und erhebliche Auswirkungen eines Sicherheitsvorfalls → Meldepflicht
  - Durchführungsrechtsakt für Meldepflicht optional

Umsetzung NIS-Richtlinie in Ö

- Netz- und Informationssystemsicherheitsgesetz (NISG)

- Novellierung Telekommunikationsgesetz:
  - RTR muss Meldung gem. § 16a Abs. 5 TKG (Sicherheitsverletzung oder Verlust der Integrität mit beträchtlichen Auswirkungen) an BMI

- Verordnungen zum NISG

NISG – Inhalt

- Einrichtung nationaler Organisations- und Koordinationsstrukturen
  - Bundeskanzler: strategische Aufgaben
  - BMI: operative Aufgaben
  - BMLVS: operativ (Defense)
- nationale NIS-Strategie
- Computer-Notfallteams (CSIRTs oder auch CERTs)

- Verpflichtungen
  - Meldung von Sicherheitsvorfällen
  - Sicherheitsvorkehrungen)
- für
  - Betreiber wesentlicher Dienste
  - Anbieter digitaler Dienste
  - Einrichtungen des Bundes
- Sanktionen

Betreiber wesentlicher Dienste - Ermittlung

- Verordnung zum NISG: Regelungen zu Sektoren
- z.B. Zahl der Nutzer, Abhängigkeit von anderen Sektoren, Marktanteil, geografische Ausbreitung, Auswirkungen von Sicherheitsvorfällen, Bedeutung des Betreibers für die Aufrechterhaltung des Dienstes, etc.
- Ermittlung Betreiber wesentlicher Dienste durch BK
- Bescheid

Pflichten für Betreiber wesentlicher Dienste

- geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen
- unverzügliche Meldung von Sicherheitsvorfällen
- Ausnahme:
  - sektorenspezifische unionsrechtliche Vorschriften mit zumindest gleichwertigem Sicherheitsniveau → Festlegung durch Verordnung
- (z.B. Zweite Zahlungsdienste-RL in Erläuterungen genannt; nicht: Meldepflicht nach DSGVO)
- freiwillige Meldung

Betreiber wesentlicher Dienste - Überprüfung

- ab 1 Jahr nach Zustellung Bescheid:
- mind. alle 3 Jahre Erfüllung der Anforderungen nachweisen
  - Aufstellung der Sicherheitsvorkehrungen durch Zertifizierungen oder Überprüfungen durch qualifizierte Stellen
- Überprüfung durch BMI jederzeit
- BMI kann Empfehlungen aussprechen

Pflichten für Anbieter digitaler Dienste

- geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen
- unverzügliche Meldung von Sicherheitsvorfällen
- Meldepflicht nur wenn Zugang zu Informationen, die benötigt werden um die Auswirkung eines Sicherheitsvorfalls zu bewerten
- freiwillige Meldung
- Überprüfung durch BMI nur im Anlassfall
- BMI kann Empfehlungen aussprechen

Sicherheitsvorfall

- Störung
  - der Verfügbarkeit
  - Integrität
  - Authentizität oder
  - Vertraulichkeit von Netz- und Informationssystemen
- Ausfall oder Einschränkung der Verfügbarkeit des Dienstes
- mit erheblichen Auswirkungen
  - betroffene Nutzer, Dauer, geografische Ausbreitung, Auswirkung auf Wirtschaft und Gesellschaft
- BMI kann nach Anhörung des BwD bzw. des AdD die Öffentlichkeit informieren
  - zur Verhütung von Sicherheitsvorfällen
  - zur Bewältigung akuter Sicherheitsvorfälle
  - im öffentlichen Interesse
  - auf Verlangen BMI hat AdD Öffentlichkeit zu informieren

Computer-Notfallteams (CSIRTs)

- Computer Security Incident Response Teams
- auch CERTs (Computer Emergency Response Teams) genannt
- cert.at, sektorenspezifische Certs, GovCert

- Entgegennahme und Weiterleitung von Meldungen von
  - Risiken, Vorfällen und Sicherheitsvorfällen
- techn. Unterstützung für betroffene Einrichtungen bei der Bewältigung von Sicherheitsvorfällen
- Handlungsempfehlungen
- Frühwarnungen

Sanktionen

- Verwaltungsstrafe bei Verstoß gegen Vorgaben NISG, z.B.
  - Meldepflicht
  - Sicherheitsvorkehrungen
  - Mitwirkungspflichten
- bis EUR 50.000
- Wiederholungsfall bis EUR 100.000
- auch gegen juristische Person möglich
- zuständig: Bezirksverwaltungsbehörde

Zusammenfassung: NIS-Richtlinie und NISG

- Sicherheit von Netz- und Informationssystemen
- betroffen:
  - Betreiber wesentlicher Dienste (kritische Infrastrukturen)
  - Anbieter digitaler Dienste
  - öffentliche Verwaltung
- Sicherheitsvorkehrungen
- Meldepflichten bei Sicherheitsvorfällen

Aufstehen,
ein „AUSSER BETRIEB“-Schild aufhängen
und alle Fragen mit
„Techniker ist informiert“
beantworten, das ist mein Plan.

WIR
SCHAUEN AUF ÖSTERREICH
WKO
WIRTSCHAFTSKAMMER ÖSTERREICH