Fact Sheet der Technologieplattform Smart Grids Austria zu NIS-Richtlinie und Datenschutzgrundverordnung

NIS Richtlinie: Network and Information Security Directive

Rechtliche Grundlage auf EU-Ebene: Directive (EU) 2016/1148 of 6th July 2016
DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures for a high common level of security of network and information systems across the Union (NIS-Directive).
https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

Ziel der Richtlinie:
Erhöhung des allgemeinen Niveaus der Netz- und Informationssicherheit für informationstechnologie-gestützte kritische Infrastrukturen und digitale Dienste, insbesondere durch verbesserte Zusammenarbeit zwischen den Mitgliedstaaten und intensivere strategische und operative Zusammenarbeit der Behörden z.B. mit Europol. Dafür werden folgende Aktivitäten angestrebt:

- verbesserte nationale Kooperation (NIS-Behörden) und Notfallteams (CSIRTs, CERTs)
- Erstellung einer Nationalen Sicherheitsstrategie und angemessenen IT-Risikomanagements
- verpflichtende Meldung signifikanter Störfälle und freiwillige Meldung für Wissensaustausch (lessons learned)
- Einrichtung eines Public-Private-Partnership Modells

für Unternehmen, die wesentliche Dienste für die Aufrechterhaltung kritischer sozialer und wirtschaftlicher Aktivitäten anbieten und stark abhängig von Netz- und Informationssystemen sind. Weiters muss deren Entfall oder die Störung des Dienstes einen signifikanten Einfluss auf die Wirtschaft oder Gesellschaft eines Mitgliedstaates oder der Europäischen Union haben.
Die NIS-Richtlinie ist keine spezielle Regelung für den Energiesektor (siehe NISRL Anhang II), sondern ein sogenanntes lex generalis.

Betroffene Stakeholder:
Betreiber wesentlicher Dienste (ersetzt den Begriff *Betreiber kritischer Infrastruktur*): Öffentliche oder private Einrichtung aus den Sektoren Energie, Verkehr, Bank- und Finanzmarktinfrastrukturen, Gesundheit, Wasserversorgung und digitale Infrastruktur
Anbieter digitaler Dienste (ausgenommen Klein- und Kleinstunternehmen):
Online-Marktplatz, Online-Suchmaschine, Cloud-Computing-Dienst
Ausgenommen: öffentliche Verwaltung, andere Sektoren (z.B. Telekommunikation), die eigenen Europäischen Richtlinien oder Verordnungen bzw. nationalen Gesetzen unterliegen.
nicht betroffen: KMU-Anbieter digitaler Dienste kleiner 50 Mitarbeiter oder Betreiber / Anbieter, welche in einem anderem Gesetz bereits den Vorgaben der Richtlinie entsprechen würden (lex specialis).

Maßnahmenkatalog:

- EU-weite Sicherheitsstandards und Zusammenarbeit zwischen den EU-Ländern
- Verpflichtende Einrichtung zuständiger Behörde(n) und Verpflichtung zur behördlichen Aufsicht
- Vorgaben für Meldepflicht signifikanter Vorfälle in Abhängigkeit von Netz- und Informations-sicherheitssystemen für Betreiber wesentlicher Dienste und Anbieter digitaler Dienste
- Unternehmen müssen technische und organisatorische Maßnahmen einrichten bzw. umsetzen
- Information anderer Mitgliedstaaten bei grenzübergreifenden signifikanten Auswirkungen

Österreichische Maßnahmen:

- Erlassung eines nationalen Gesetzes zur Umsetzung der NIS-Richtlinie
- Meldewege für verpflichtende und freiwillige Meldungen, Schwellwerte für Meldeverpflichtungen
- Identifikation von Betreibern wesentlicher Dienste per Bescheid
- Sicherheitsanforderungen bzw. Normierungsmöglichkeiten für Betreiber, Sanktionen festlegen
- Einrichtung von NIS-Behörde(n) und eines SPoCs als Ansprechpartner für andere Mitgliedstaaten und im Public-Private-Partnership Modell
- Etablierung des Branchen-CERTs im EU-CSIRT-Netzwerk und im nationalen CERT-Verbund als koordinierende Meldestelle zu der/n NIS-Behörde/n bzw. zur nationalen Kooperationsgruppe
- Horizontale und vertikale Kommunikationswege aufbauen bzw. verbessern im Falle eines Ausfalls von Energie (Blackout) oder auch von Telekommunikationseinrichtungen (Internet)

Zeitplan der Umsetzung der NIS Richtlinie auf nationaler Ebene:

- Die EU-Richtlinie Directive (EU) 2016/1148 ist seit 8. August 2016 in Kraft
- Bis 9. Mai 2018 sind entsprechende Vorschriften zu erlassen, um die NISRL national umzusetzen
- Ab dem 10. Mai 2018 soll das nationale Gesetz zur NISRL in Kraft treten
- Bis 9. November 2018 müssen die betroffenen Unternehmen ermittelt worden sein

Datenschutzgrundverordnung: General Data Protection Regulation

Rechtliche Grundlage auf EU-Ebene:
General Data Protection Regulation 2016/679 vom 27.4.2016.
http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE

Mit der vom Europäischen Parlament beschlossenen Datenschutzgrundverordnung werden die Regeln für die Verarbeitung personenbezogener Daten, die Rechte der Betroffenen und die Pflichten der Verantwortlichen EU-weit vereinheitlicht.
Die Datenschutzgrundverordnung ist zwar als EU-Verordnung in jedem EU-Mitgliedstaat unmittelbar anwendbar, sie lässt dem nationalen Gesetzgeber jedoch gewisse Spielräume. Es wird daher auch eine Änderung des österreichischen Datenschutzgesetzes 2000 geben.

Ziel der Verordnung:
Mit der Verordnung wird das Datenschutzrecht EU-weit vereinheitlicht und das Grundrecht zum Schutz personenbezogener Daten von natürlichen Personen nach der Charta der Grundrechte Artikel 8 angewandt. Dadurch soll einerseits der Schutz von personenbezogenen Daten innerhalb der Europäischen Union sichergestellt, andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.

Betroffene Stakeholder:
Die Datenschutzgrundverordnung betrifft jedes Unternehmen mit über 250 Mitarbeitern, das personenbezogene Daten erfasst oder verarbeitet.

Maßnahmenkatalog:
- Befugnisse und Aufgaben der Aufsichtsbehörden werden erweitert
- Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen („privacy by design/ privacy by default“)
- Stärkung der Betroffenenrechte (mehr Transparenz; Verankerung des Rechts auf „Vergessen werden“; Einwilligung gilt nur falls freiwillig, aktiv und eindeutig)
- Neuer Fokus auf die Datensicherheit (verpflichtende angemessene Sicherheitsvorkehrungen; Datenmissbräuche und Sicherheitsverletzungen müssen den Aufsichtsbehörden gemeldet werden)
- Meldungen von Verletzungen des Schutzes personenbezogener Daten sind sowohl den nationalen Aufsichtsbehörden als auch der betroffenen Person mitzuteilen
- Verantwortliche und Auftragsverarbeiter müssen ein „Verzeichnis von Verarbeitungstätigkeiten“ führen, Pflicht zur Datenschutz-Folgenabschätzung bei Verarbeitungsvorgängen
- Verpflichtung zur Bestellung eines Datenschutzbeauftragten besteht für Unternehmen
- Verschärfungen der Anforderungen bei Übermittlung an Drittstaaten und grenzüberschreitender Datenverarbeitung
- Hohe Strafen von bis zu 20 Mio. Euro oder im Fall eines Unternehmens von bis zu 4 % seines weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres für Verantwortliche oder Auftragsverarbeiter

Österreichische Maßnahmen:
- Festlegung der Kriterien für Datenschutzbeauftragte in den Unternehmen
- Umsetzung in nationales Recht durch Änderung des Datenschutzgesetzes 2000 und Bearbeitung von Öffnungsklauseln
- Festlegung von technischen und organisatorischen Maßnahmen, z.B. bei Smart Meter Systemen
- Zuständigkeitszuweisungen
- Grenzwertfestsetzungen für Strafen bei Verletzung der Verordnung

Zeitplan der Umsetzung der Datenschutzgrundverordnung auf nationaler Ebene:
- Erlass der General Data Protection Regulation 2016/679 vom 27.4.2016
- Die Datenschutz-Grundverordnung tritt am 25. Mai 2018 in Geltung

Kontaktdaten
Dr. Angela Berger, Geschäftsführerin
Technologieplattform Smart Grids Austria
1060 Wien, Mariahilfer Straße 37-39
E: angela.berger@smartgrids.at
I: www.smartgrids.at

Abkürzungen
CERT … Computer Emergency Response Team
CSIRT … Computer Security Incident Response Teams
SPoC … Single Point of Contact