

Netzintegrität und Netzsicherheit: Einführung in die Thematik

Ulrich Latzenhofer
Technik



Motivation

- Zentrale Bedeutung zuverlässiger und sicherer Kommunikation für Wirtschaft und Gesellschaft
- Auswirkungen von Systemkomplexität, Ausfällen, Bedienungsfehlern, Unfällen und vorsätzlichen Eingriffen auf Funktion und Verfügbarkeit von IKT-Infrastruktur
- Umzusetzende Vorgaben aus Telekom-Paket:
Auftrag an nationale Regulierungsbehörden, Aufrechterhaltung von Integrität und Sicherheit öffentlicher Kommunikationsnetze sicherzustellen
- Sicherheit als ständiger Prozess:
Durchführung – Überprüfung – Aktualisierung
- Maßnahmen zum Schutz von Integrität und Sicherheit im Einklang mit Risikobeurteilung unter Berücksichtigung des Stands der Technik



§ 16a TKG 2003: Neue Pflichten der Betreiber

Maßnahmen

- Integrität von Netzen und fortlaufende Verfügbarkeit von Diensten
- Sicherheitsniveau zur Beherrschung der Risiken für Netzsicherheit

Informationspflichten

- gegenüber Regulierungsbehörde
 - Informationen zur Beurteilung von Sicherheit und Integrität (nach Aufforderung)
 - Mitteilungen über Sicherheitsverletzungen und Integritätsverluste mit beträchtlichen Auswirkungen
- gegenüber Öffentlichkeit (nach Aufforderung)

Sicherheitsüberprüfung

- bei Vorliegen konkreter Anhaltspunkte für Gesetzesverstoß (auf Anordnung der Telekom-Control-Kommission)
- auf Kosten der betroffenen Betreiber



§ 16a TKG 2003: Tätigkeit der Regulierungsbehörde

Bearbeitung von Mitteilungen über Vorfälle

- Festlegung der Form von Mitteilungen
- Information der Öffentlichkeit, falls Bekanntgabe im öffentlichen Interesse liegt
- ggf Weitergabe von Informationen an ENISA und Regulierungsbehörden anderer Mitgliedstaaten
- jährlicher zusammenfassender Bericht an Europäische Kommission und ENISA

Gegebenenfalls Beurteilung übermittelter Informationen (zB Unterlagen über Sicherheitsmaßnahmen)

Sicherheitsüberprüfungen: Durchführung durch Regulierungsbehörde oder beauftragte qualifizierte unabhängige Stelle

Abstimmung mit Datenschutzkommission: je nach Zuständigkeit



Tätigkeit der ENISA

Europäische Agentur für Netz- und Informationssicherheit
2004 als Institution der EU eingerichtet, Sitz in Iraklio



Allgemeine Aufgaben (Beispiele)

- Unterstützung von Einrichtungen der EU und der Mitgliedstaaten
- Förderung der Zusammenarbeit zwischen verschiedenen Akteuren
- Sensibilisierung und Informationsvermittlung

Relevante Aufgaben bezüglich Netzintegrität und Netzsicherheit

- Entgegennahme von Berichten über Sicherheitsverletzungen und Integritätsverluste
- Stellungnahme bei Erlass technischer Durchführungsmaßnahmen durch Europäische Kommission
- Technische Leitlinien zur Harmonisierung (eventuell Grundlage einer künftigen Verordnung nach § 16a Abs 9 TKG 2003)



Technical Guideline on Minimum Security Measures

- Aufstellung der von Betreibern zu ergreifenden Sicherheitsmaßnahmen
- Gliederung in sieben Bereiche mit insgesamt 26 Unterbereichen
 - Risikomanagement
 - Sicherheit bezüglich Personal
 - Sicherheit von Systemen und Betriebsstätten
 - Betriebsmanagement
 - Störfallmanagement
 - Betriebliches Kontinuitätsmanagement
 - Monitoring, Audits, Tests
- Nur exemplarische Sicherheitsmaßnahmen konkret genannt (Beispiele aus internationalen Standards, zB ISO/IEC 27011)
- <http://www.enisa.europa.eu/act/res/reporting-incidents/minimum-security-requirements/technical-guideline-on-minimum-security-measures>



Technical Guideline on Reporting Incidents

- Technische Leitlinie für jährlichen zusammenfassenden Bericht nationaler Regulierungsbehörden an Europäische Kommission und ENISA
- Festlegung, welche Angaben über jeden Vorfall in den Bericht aufzunehmen sind
- Auslegung des Begriffs „beträchtliche Auswirkungen“
⇒ Festlegung von Schwellwerten, die Berichtspflicht auslösen
- Bedeutsam für Anwendung relevanter Rechtsvorschriften in Österreich (insbesondere Mitteilungen der Betreiber an Regulierungsbehörde)
- <http://www.enisa.europa.eu/act/res/reporting-incidents/incidents-reporting-to-enisa/technical-guideline-on-incident-reporting>



Zusammenfassung

- Konkretisierung von Pflichten der Betreiber nach § 16a TKG 2003 in einer noch zu erlassenden Verordnung des BMVIT
- Vorläufige Grundlage: Technical Guidelines der ENISA
 - Ziel: Harmonisierung des Sicherheitsniveaus
 - Von Mitgliedstaaten der EU getragen
 - Österreichische Betreiber im Wege ihrer Interessenvertretungen beteiligt
 - Voraussichtlich Berücksichtigung in Verordnung des BMVIT
- Zweck des heutigen Workshops: gemeinsames Verständnis
 - Technical Guidelines der ENISA
 - Informationspflichten der Betreiber
 - Geeignete Sicherheitsmaßnahmen

Netzintegrität und Netzsicherheit

Ulrich Latzenhofer
Technik