Wir stehen für **Wettbewerb** und **Medienvielfalt**.

Rundfunk & Telekom Regulierungs-GmbH
RTR

Aktualisierte technische Leitlinien der ENISA

Mag. Ulrich Latzenhofer

RTR-GmbH

10. Oktober 2013

Artikel 13a und 13b Rahmenrichtlinie

Maßnahmen der Betreiber

- Integrität der Netze, Verfügbarkeit der Dienste
- Beherrschung der Risiken für die Netzsicherheit

Informationspflichten (Mitteilung von Vorfällen)

Harmonisierungsmaßnahmen der Europäischen Kommission (?)

Anordnungen der nationalen Regulierungsbehörde (kurz NRB)

- Übermittlung von Informationen zur Beurteilung von Sicherheit/Integrität
- Sicherheitsüberprüfung auf Kosten des Betreibers

Tätigkeit der ENISA

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

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

Technical Guideline on Minimum Security Measures, Version 1.0

Zusammenstellung von Sicherheitszielen und -maßnahmen

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, z. B. ISO/IEC 27001)

Technical Guideline on Security Measures, Version 2.0

Version 1.0 nach wie vor aktuell

Version 1.93 als Entwurf für Version 2.0 veröffentlicht

Unterschiede zu Version 1.0

- 25 Sicherheitsziele in sieben Bereichen
- Mehrere konkrete Sicherheitsmaßnahmen pro Sicherheitsziel
- Sophistication levels (Vollkommenheitsgrade):
  Basic (1) – Industry standard (2) – State of the art (3)
- Individuelle Festlegung des Sophistication levels für jedes Sicherheitsziel
- Zuordnung jeder Sicherheitsmaßnahme zu einem Sophistication level
- Nachweis von Sicherheitsmaßnahmen

Beispiel: Sicherheitsmaßnahmen zu einem Sicherheitsziel

Security objective 23: Network and information systems testing

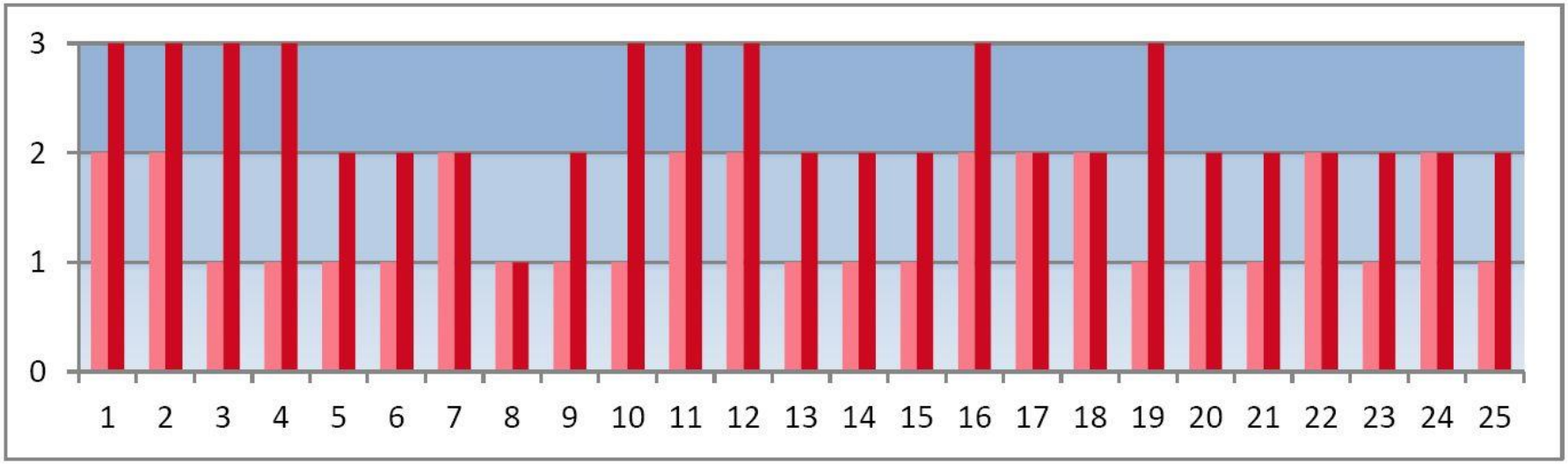
	Security measures	Evidence
1	a) Test networks and information systems before using them or connecting them to existing systems	• Test reports of the network and information systems, including tests after big changes or the introduction of new systems
2	b) Implement policy/procedures for testing network and information systems c) Implement tools for automated testing	• Policy/procedures for testing networks and information systems, including when tests must be carried out, test plans, test cases, test report templates
3	d) Review and update the policy/procedures for testing, taking into account changes and past incidents	• Inventory of test reports • Updated policy/procedures for testing networks and information systems • Review comments, change log

Selbsteinschätzung des Betreibers

Zu berücksichtigende Faktoren

- Risiko (abhängig u. a. von der Unternehmensgröße)
- Bereits getroffene Sicherheitsmaßnahmen
- Aufwand der noch zu treffenden Sicherheitsmaßnahmen

Profile: Sophistication levels für verschiedene Sicherheitsziele



Technical Guideline on Reporting Incidents, Version 1.0

Einheitliche Vorgaben für jährlichen zusammenfassenden Bericht von NRB 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)

Technical Guideline on Incident Reporting, Version 2.0

Version 2.0 im Jänner 2013 veröffentlicht

Unterschiede zu Version 1.0

- Vereinfachung und Kürzung (von 38 auf 21 Seiten)
- Präzisere Formulierungen
  z. B. Definition „Affected users“ auf Basis Teilnehmer bzw. SIM-Karten
- Kriterien für „beträchtliche Auswirkungen“
  Region und geographische Ausbreitung nicht mehr relevant
  Dauer und Anteil der betroffenen Nutzer weiterhin relevant
  Optionaler Schwellwert: 3 Mio. Nutzerstunden
  Dienste: nur Unterscheidung zwischen fest/mobil, Telefonie/Internet
- Zusätzliche Felder im Formular
  „Initial cause“ und „Subsequent cause“
  Optionale Information zu Technologie bzw. Plattform

Umsetzung in Österreich: Kriterien für Mitteilungspflicht

Mitteilungspflicht nur bei „beträchtlichen Auswirkungen“

- Notrufnummern nicht erreichbar (vgl. Vortrag Schramm/Weber) oder
- Dienst nicht verfügbar und Schwellwerte überschritten

Aktuelle Schwellwerte auf Website der RTR-GmbH

Voraussichtliche Schwellwerte ab 2014

Dienstekategorie \ Dauer	*> 1 h*	*> 2 h*	*> 4 h*	*> 6 h*	*> 8 h*
Festnetztelefonie	400.000	270.000	130.000	50.000	30.000
Mobiltelefonie	2.000.000	1.400.000	700.000	300.000	100.000
Feste Internetzugänge	330.000	220.000	110.000	40.000	20.000
Mobile Internetzugänge	730.000	490.000	240.000	100.000	50.000

Umsetzung in Österreich: Mitteilungen an die RTR-GmbH

Formular derzeit auf Website der RTR-GmbH

Integration in eRTR ab 2014

Unverzügliche Mitteilung an RTR-GmbH

- Sobald beträchtliche Auswirkungen absehbar
- Vervollständigung zu späterem Zeitpunkt möglich
- Unternehmensinterner Prozess ggf. anzupassen

Links

Relevante Informationen der ENISA
einschließlich technischer Leitlinien
https://resilience.enisa.europa.eu/article-13

Relevante Informationen der Regulierungsbehörde
einschließlich des Mitteilungsformulars
https://www.rtr.at/de/tk/Netzsicherheit

Präsentationen des Workshops
https://www.rtr.at/de/komp/Workshop10102013

Wir stehen für **Wettbewerb** und **Medienvielfalt**.

Rundfunk & Telekom Regulierungs-GmbH
RTR

Aktualisierte technische Leitlinien der ENISA

Mag. Ulrich Latzenhofer

RTR-GmbH

10. Oktober 2013