Ein Sicherheitsniveau für Netze und Dienste

Aus der Praxis zu § 44 TKG 2021

Ulrich Latzenhofer

Inhalt

- Ein Sicherheitsniveau …
- Aufgaben der Regulierungsbehörde
- Sicherheitsmaßnahmen
  (Guideline der ENISA, 5G-Netze, Branchenrisikoanalyse)
- Meldung von Sicherheitsvorfällen
  (Meldewege, Kriterien für Meldepflicht, Statistik und Trends)

Ein Sicherheitsniveau …

- Technische und organisatorische Maßnahmen
  - Sicherheitsniveau zur angemessenen Beherrschung der Risiken für die Sicherheit von Netzen und Diensten
  - Berücksichtigung des Standes der Technik
  - Sicherheitsniveau angesichts des bestehenden Risikos verhältnismäßig und angemessen
- Risiken und Maßnahmen abhängig von Betreiber/Anbieter
- Potenzielle Auswirkungen von Sicherheitsvorfällen auf andere Netze/Dienste → gemeinsames Sicherheitsniveau
- Durchsetzung durch Regulierungsbehörde

Aufgaben der Regulierungsbehörde (1)

Aufgabe	Zuständig	Grundlage
Anordnung einer Sicherheitsüberprüfung (bei Anhaltspunkten für unzureichende Sicherheitsmaßnahmen)	TKK	§ 44 Abs 4
Beurteilung der Sicherheit anhand übermittelter Informationen des Betreibers/Anbieters	RTR	§ 44 Abs 3
Anordnung von Maßnahmen	RTR	§ 44 Abs 1 § 184 Abs 2, 4
Äußerstenfalls Entzug der Berechtigung zur Bereitstellung von Netzen/Diensten	TKK	§ 184 Abs 3

Aufgaben der Regulierungsbehörde (2)

Aufgabe	Zuständig	Grundlage
Entgegennahme von Mitteilungen über Sicherheitsvorfälle	RTR	§ 44 Abs 5
Weiterleitung von Mitteilung an BMI	RTR	§ 44 Abs 6
Information der Regulierungsbehörden anderer MS oder der ENISA über Sicherheitsvorfall	RTR	§ 44 Abs 7
Information der Öffentlichkeit über Sicherheitsvorfall	RTR	§ 44 Abs 8
Jährlicher zusammenfassender Bericht an EK und ENISA	RTR	§ 44 Abs 9

Aufgaben der Regulierungsbehörde (3)

Aufgabe	Zuständig	Grundlage
Verordnung zu § 44 Abs 1 und 5	RTR	§ 44 Abs 10
Abstimmung mit DSB	RTR	§ 44 Abs 12
Beiziehung von Computer-Notfallteams, Abstimmung mit Behörden gemäß NISG	RTR	§ 44 Abs 13
Zuständigkeit für alle Aufgaben in Bezug auf Medien	KOA	§ 44 Abs 11 § 199 Abs 2 Z 9

Aufgaben der RTR gemäß TK-NSiV 2020

Aufgabe	Grundlage
Betrieb des Meldeportals für Sicherheitsvorfälle	§ 3 Abs 1, § 4 Abs 2
Veröffentlichung von Daten zur Ermittlung der Schwellwerte	§ 3 Abs 4
Entgegennahme freiwilliger Warnhinweise	§ 4 Abs 1
Beurteilung von Auditberichten für ISMS	§ 6 Abs 1
Beurteilung von Konformitätserklärungen zu 5G-Standards	§ 6 Abs 2
Beurteilung der Erfüllung besonderer 5G-Anforderungen	§ 6 Abs 3
Beurteilung der Aufstellung von Funktionen und Herstellern eingesetzter 5G-Komponenten	§ 6 Abs 4

Relevante Neuerungen im TKG 2021

§ 16a TKG 2003	§ 44 TKG 2021
Umsetzung Art 13a, 13b RahmenRL	Umsetzung Art 40, 41 EECC
Sicherheit und Integrität von Netzen/Diensten	Sicherheit von Netzen/Diensten (Integrität nur in Überschrift)
Integrität von Netzen als Voraussetzung für Verfügbarkeit von Diensten	Integrität neben Verfügbarkeit, Authentizität, Vertraulichkeit (Schutzziele der Informationssicherheit) Teilaspekt der Sicherheit von Netzen/Diensten
Dienste: Übertragung von Signalen (auch Rundfunk)	Internetzugangsdienste, interpersonelle Kommunikationsdienste (auch OTT), Übertragung von Signalen (auch M2M, Rundfunk)
Meldepflicht bei Vorfällen mit „beträchtlichen Auswirkungen“: quantitative Kriterien Dauer und Anzahl betroffener Teilnehmer, vgl TK-NSiV 2020	Zusätzlich qualitative Kriterien: geographische Ausdehnung, Ausmaß der Beeinträchtigung des Netzes/Dienstes, Ausmaß der wirtschaftl/gesellschaftl Auswirkungen

Sicherheitsmaßnahmen

- ENISA Guideline on Security Measures under the EECC (2021)
- Weiterentwicklung der ENISA Technical Guideline on Security Measures seit 2011
- Konsens zuständiger Behörden der EWR-Staaten im Rahmen der ENISA ECASEC Expert Group
- 29 Sicherheitsziele in 8 Bereichen
- Zu jedem Sicherheitsziel Maßnahmen und zugehörige Nachweise in drei Vollkommenheitsgraden („basic“, „industry standard“, „state of the art“)

Sicherheitsmaßnahmen: Bereiche nach ENISA

D1: GOVERNANCE AND RISK MANAGEMENT
- SO1: Information security policy
- SO2: Governance and risk management
- SO3: Security roles and responsibilities
- SO4: Security of third party dependencies

D2: HUMAN RESOURCES SECURITY
- SO5: Background checks
- SO6: Security knowledge and training
- SO7: Personnel changes
- SO8: Handling violations

D3: SECURITY OF SYSTEMS AND FACILITIES
- SO9: Physical and environmental security
- SO10: Security of supplies
- SO11: Access control to network and information systems
- SO12: Integrity of network and information systems
- SO13: Use of encryption
- SO14: Protection of security critical data

D4: OPERATIONS MANAGEMENT
- SO15: Operational procedures
- SO16: Change management
- SO17: Asset management

D5: INCIDENT MANAGEMENT
- SO18: Incident management procedures
- SO19: Incident detection capability
- SO20: Incident reporting and communication

D6: BUSINESS CONTINUITY MANAGEMENT
- SO21: Service continuity strategy and contingency plans
- SO22: Disaster recovery capabilities

D7: MONITORING, AUDITING AND TESTING
- SO23: Monitoring and logging policies
- SO24: Exercise contingency plans
- SO25: Network and information systems testing
- SO26: Security assessments
- SO27: Compliance monitoring

D8: THREAT AWARENESS
- SO28: Threat intelligence
- SO29: Informing users about threats

Sicherheit von 5G-Netzen

- Erhöhte Angriffsgefahr und mehr potenzielle Ansatzpunkte für Angreifer, leichtere Verwundbarkeit bestimmter Netzkomponenten und -funktionen
- Erhöhte Risiken durch größere Abhängigkeit von Lieferanten, potenzieller Einfluss von Nicht-EU-Ländern auf Lieferanten

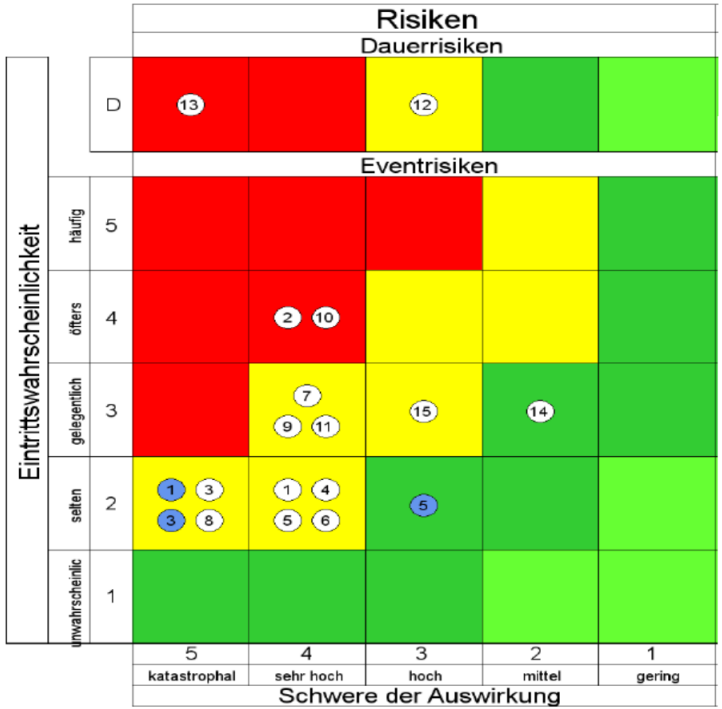
Besondere Aktivitäten auf europäischer Ebene

- Koordinierte Risikoanalyse der Cybersicherheit von 5G-Netzen (2019)
- EU-Instrumentarium der Risikominderungsmaßnahmen („Toolbox“, 2020)
- 5G Supplement zur ENISA Guideline on Security Measures (2021)
- Umsetzung technischer Maßnahmen in Österreich durch § 6 TK-NSiV 2020

Branchenrisikoanalysen

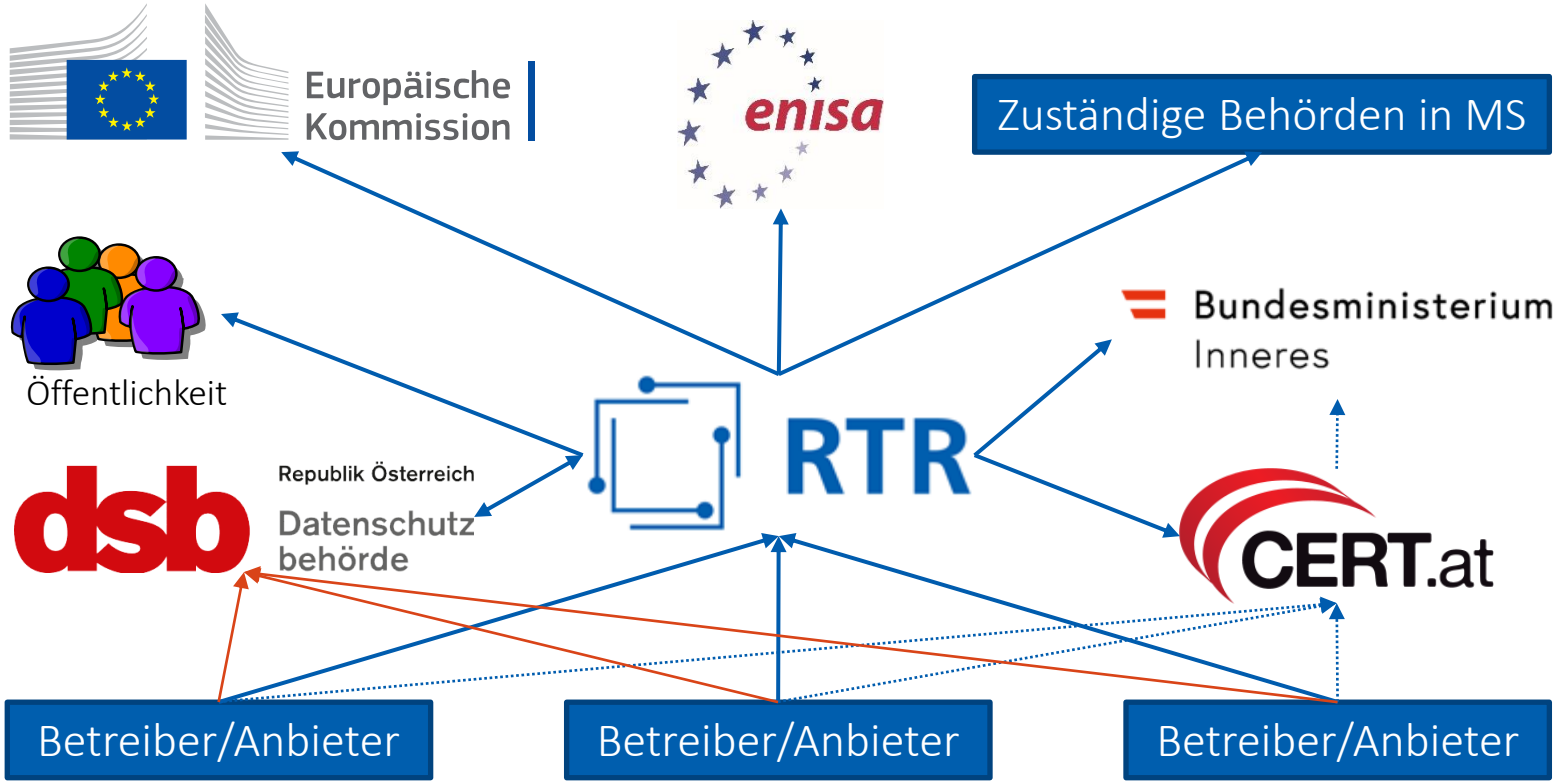
- Grundlagen für branchenspezifische Risikoanalysen in ÖSCS (2013), APCIP, künftig auch NIS-2-RL
- Kooperation mit Betreibern, Ministerien und anderen Stakeholdern unter Federführung der RTR seit 2017
- Strukturierter Prozess (Lenkungsausschuss, techn Expertengremium)
- Vollständige Risikoanalysen 2018 und 2020, 5G-Risiken 2019
- Maßnahmen/Empfehlungen für Betreiber kritischer Infrastrukturen, systemrelevante Betreiber, Behörden und Sonstige
- Wechselwirkungen mit anderen Branchen (Kaskadeneffekte): seit 2020 verstärkte Kooperation mit Energiewirtschaft

Branchenrisikoanalyse 2020



- 13, Verwundbarkeiten bei Hard- und Software
- 02, Vorsätzliche Beschädigung, Zerstörung, Diebstahl wichtiger Betriebsmittel
- 10, Vertraulichkeitsverlust von geschützten Informationen
- 12, Mängel in der Betriebsführung
- 07, Mangelhaftes Notfall-, Krisen- und Kontinuitäts-Management
- 09, Defizite bei Identity and Access Management (IAM)
- 11, Ausfall oder erhebliche Serviceeinschränkungen bei/von singulären IKT-Lieferanten
- 03, Kriminelle Handlungen aus dem Cyberraum
- 08, Erhebliche Probleme beim Patch- und Updateprozess
- 01, Ausfall wesentlicher Infrastrukturen
- 04, Mögliche erhebliche Defizite bei IKT-Designfragen
- 05, Negative Auswirkungen von politisch-rechtlichen Rahmenbedingungen
- 06, Defizite im Beschaffungsprozess
- 15, Ausfall wesentlicher Betriebsmittel, insbesondere Strom

Sicherheitsvorfälle: Meldewege



Sicherheitsvorfälle: Meldeschwellen ENISA

- Absoluter Schwellert: Dauer × # Nutzer > 1 Mio Nutzerstunden
- Relative Schwellwerte:

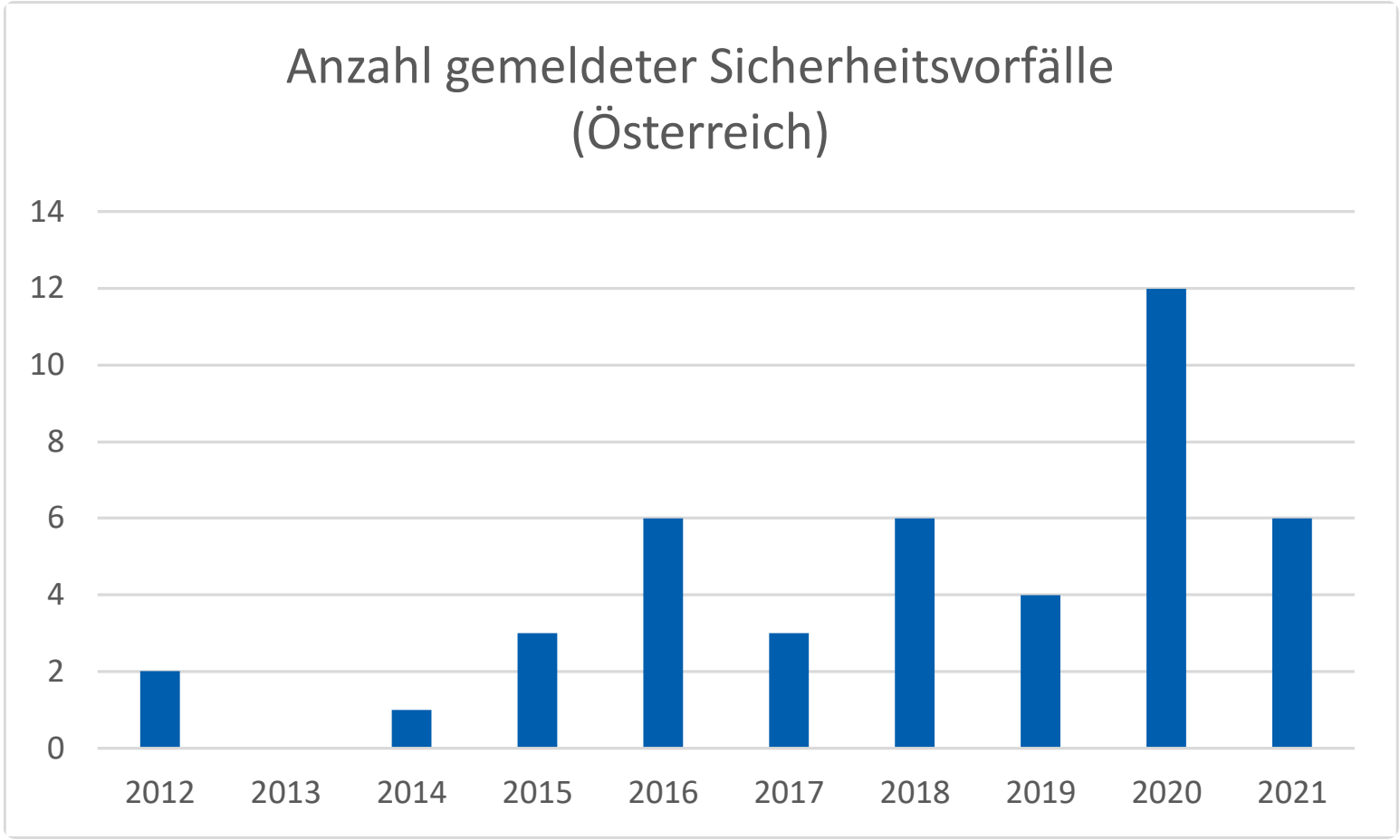
	1h–2h	2h–4h	4h–6h	6h–8h	> 8h
1%–2%					
2%–5%					
5% –10%					
10%–15%					
> 15%					

Quelle: ENISA

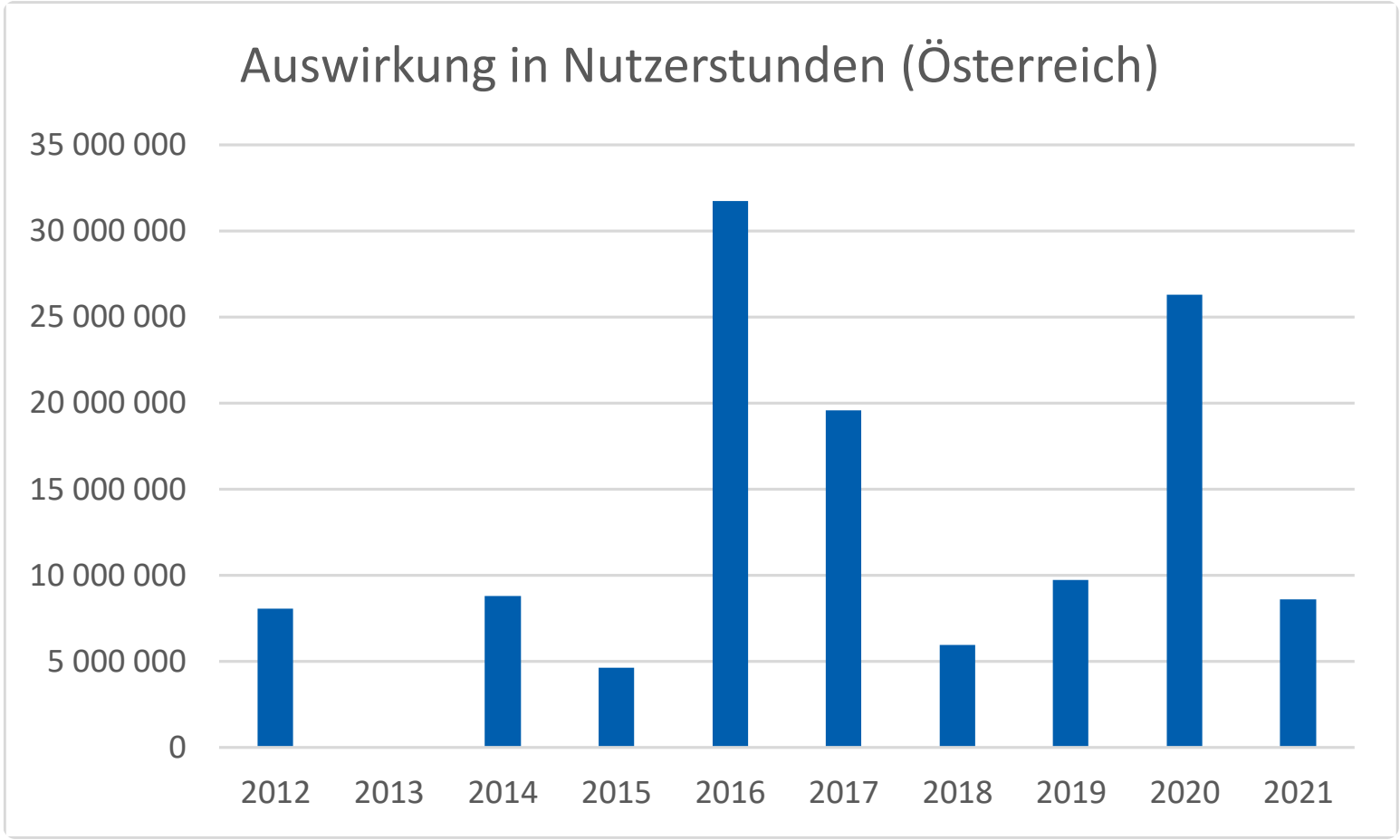
Sicherheitsvorfälle: Meldeschwellen RTR

- Zusammenfassung von absolutem und relativen Schwellwerten in § 3 Abs 2 TK-NSiV 2020
- Umrechnung in absolute Zahlen für verschiedene Kategorien von Diensten auf Website der RTR

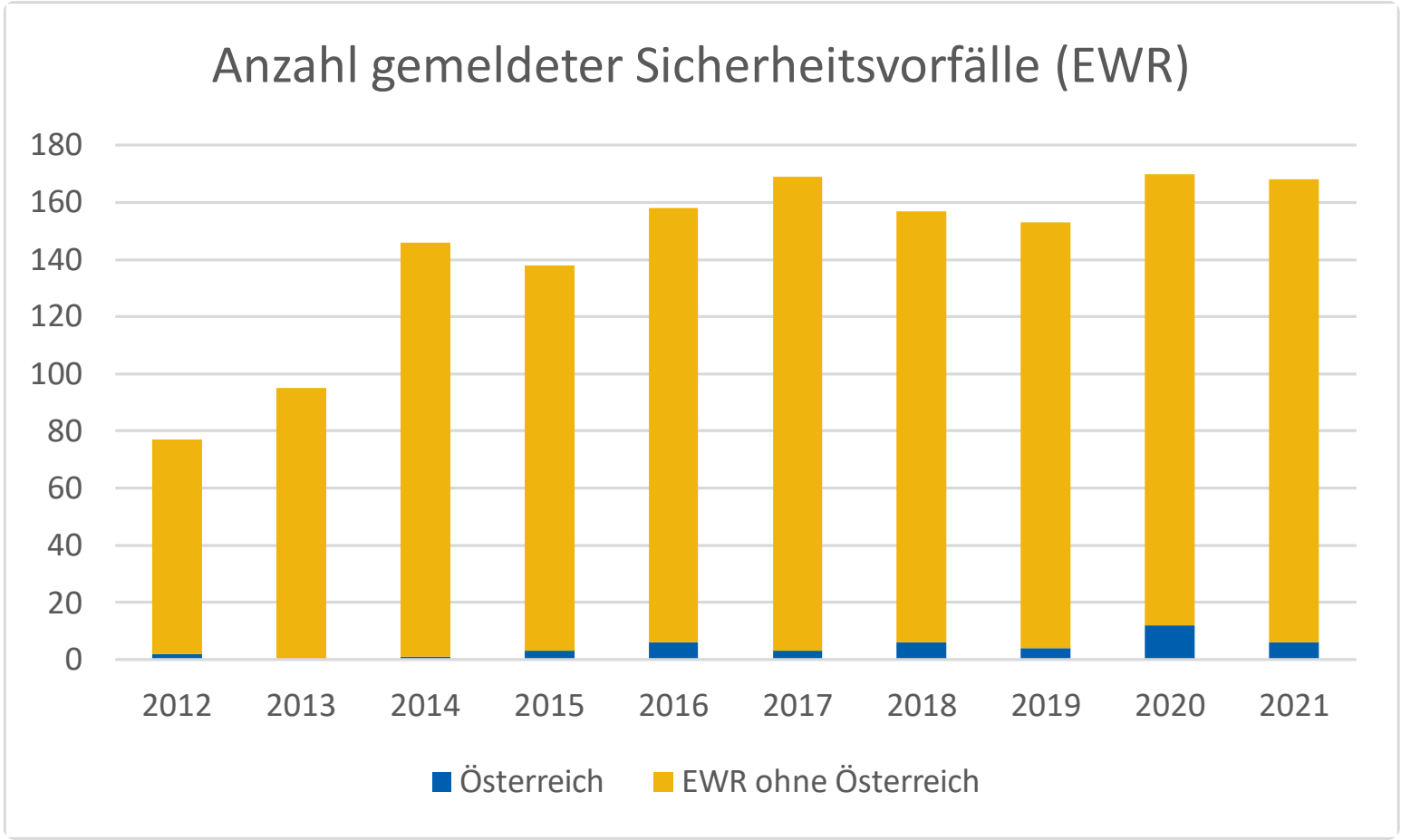
Dienstekategorie/Dauer	≤ 1 h	> 1 h	> 2 h	> 4 h	> 6 h	> 8 h	> 16 h
Nummerngebundene interpersonelle Kommunikationsdienste							
Fester Sprachkommunikationsdienst	500.000	340.000	230.000	110.000	50.000	20.000	10.000
Mobiler Sprachkommunikationsdienst	500.000	500.000	250.000	150.000	100.000	50.000	10.000
Nummerngebundener Nachrichtendienst (SMS)	500.000	500.000	250.000	150.000	100.000	50.000	10.000
Internetzugangsdienste							


Anzahl gemeldeter Sicherheitsvorfälle (Österreich)
14
12
10
8
6
4
2
0
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021

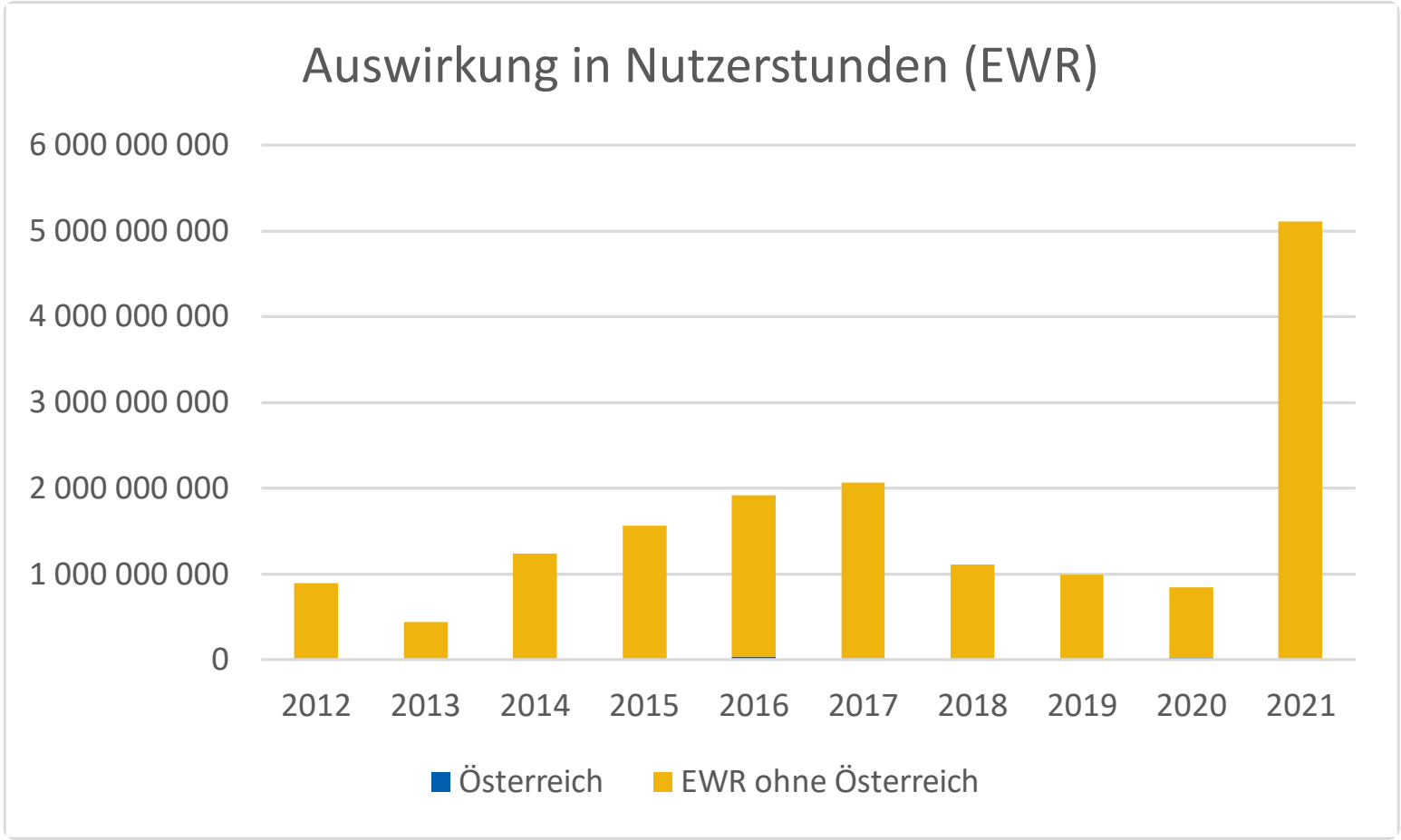
Quelle: RTR


Auswirkung in Nutzerstunden (Österreich)
35 000 000
30 000 000
25 000 000
20 000 000
15 000 000
10 000 000
5 000 000
0
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021

Quelle: RTR

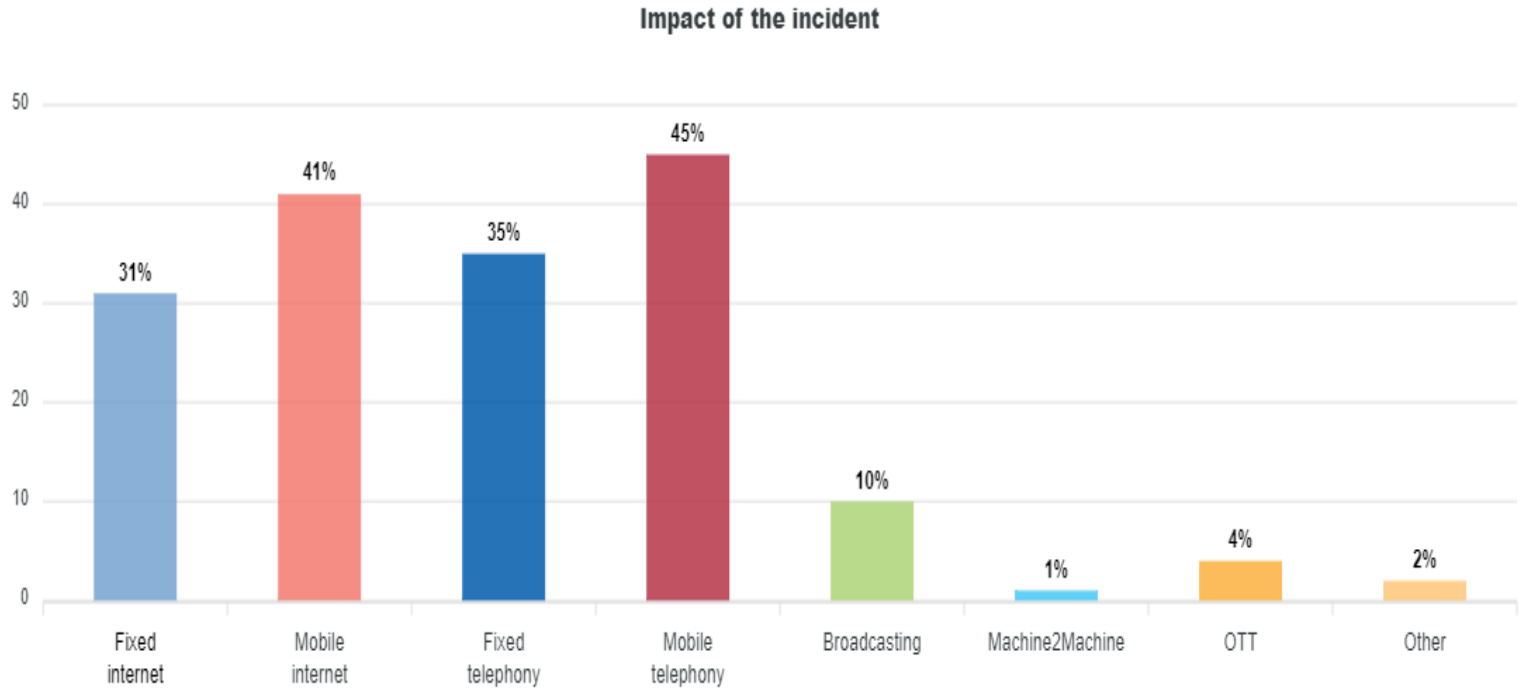


Quelle: RTR, ENISA



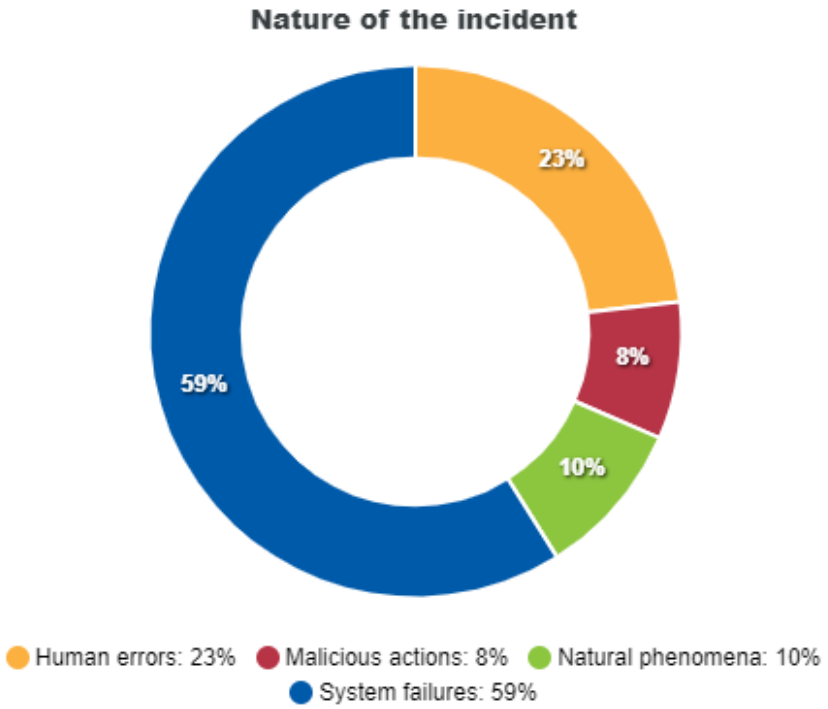
Quelle: RTR, ENISA

Sicherheitsvorfälle: betroffene Dienste 2021



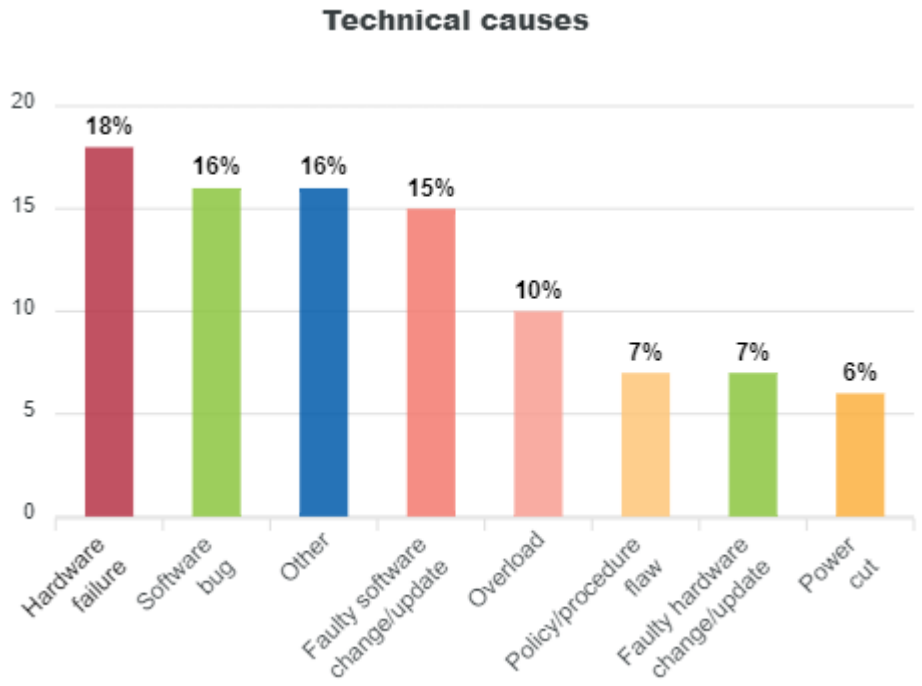
Quelle: ENISA

Sicherheitsvorfälle: Grundursachen 2021



Quelle: ENISA

Sicherheitsvorfälle: technische Ursachen 2021



Quelle: ENISA

Sicherheitsvorfälle: Zusammenfassung

- Anzahl gemeldeter Vorfälle auf nationaler Ebene stark schwankend, auf europäischer Ebene tendenziell gleichbleibend
- Auswirkung von Vorfällen überwiegend bei OTT-Diensten (trotz geringer Anzahl solcher Vorfälle)
- Auch Vorfälle betreffend Vertraulichkeit und Authentizität meldepflichtig (2021 auf europäischer Ebene drei solcher Vorfälle gemeldet)
- Anzahl böswilliger Handlungen stark steigend (2021 Verdoppelung von 4 auf 8 Prozent aller Vorfälle, vor allem DDoS-Angriffe)
- Auswirkung von Systemfehlern in Relation zur Gesamtauswirkung abnehmend
- Anteil der Vorfälle wegen menschlichen Versagens etwa gleichbleibend
- Anteil der Vorfälle wegen Drittversagens abnehmend

RTR

Wir stehen für Wettbewerb und Medienvielfalt

Auf Wiedersehen!

RTR-GmbH, Mariahilfer Straße 77 – 79, 1060 Wien | www.rtr.at