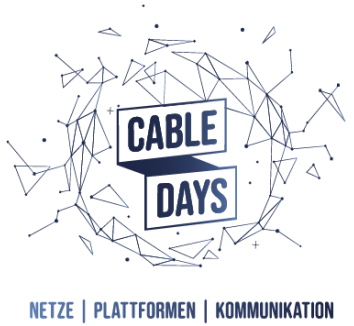



Dr. Natalie Ségur-Cabanac

# Network Information Security

## Aus dem Blickwinkel von Telekommunikationsunternehmen

Design Center Linz

24. und 25. Oktober 2023

WKO Telekom·Rundfunk

# Die ISPA vertritt die Internetwirtschaft

- **Gegründet 1997**
- **220 Mitglieder aus den Bereichen**
  - Access
  - Hosting
  - Content & Services
- **Zwei Drittel der Mitglieder KMUs**

**ISPA - MISSION STATEMENT**

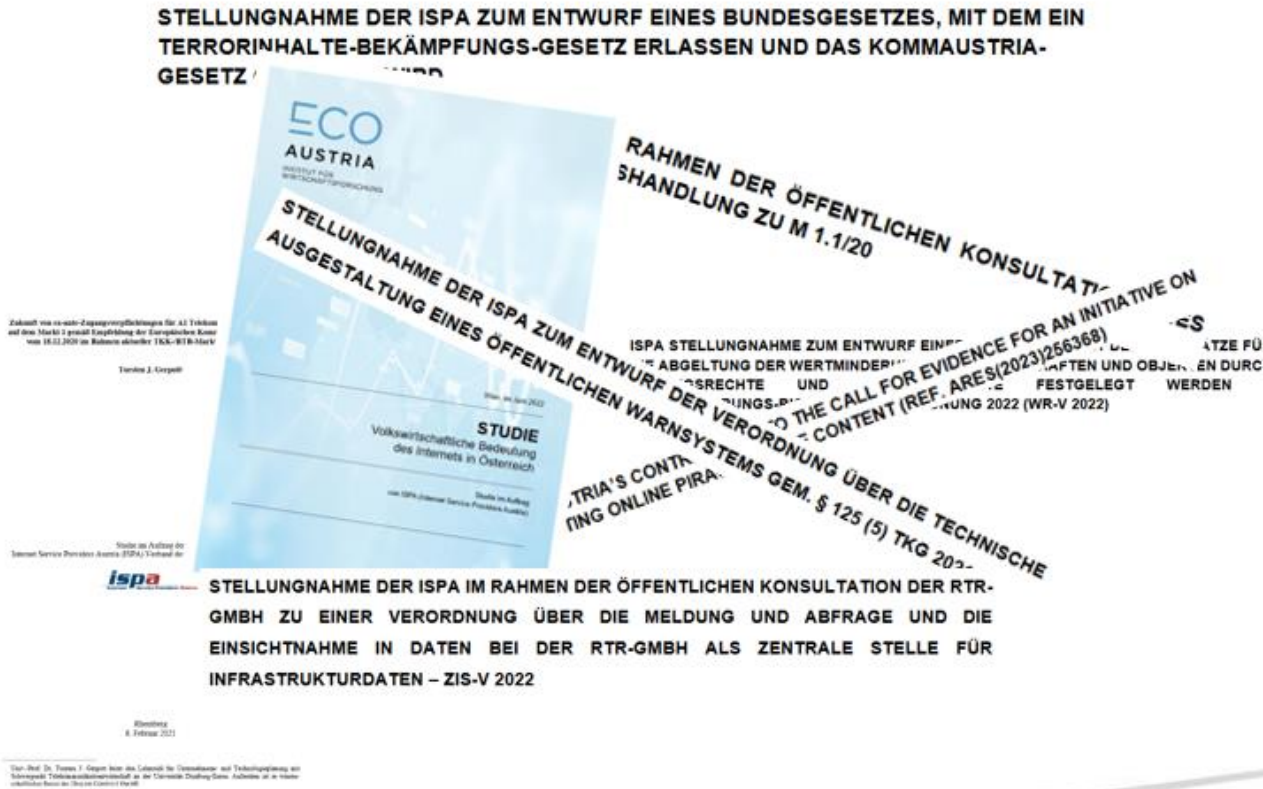
Als Interessensvertretung der Internetwirtschaft sehen wir in der Nutzung digitaler Technologien die Grundlage für eine gesunde Wirtschaft und eine fortschrittliche Gesellschaft. Wir fördern und fordern daher nachdrücklich optimale Rahmenbedingungen für die digitale Zukunft und nehmen die daraus entstehende gesellschaftspolitische Verantwortung wahr.

ispa Internet Service Providers Austria

# Interessensvertretung

- **ISPA Arbeitsgruppen**
  - Access
  - Content & Services
  - Security
  - Recht
  - Datenschutz

- **Positionierung Politik & Verwaltung**
  - Gutachten, Studien
  - Stellungnahmen & Eingaben
  - regelm. Austausch




ispa
Internet Service Providers Austria

# Mitgliederservice

- **Beratung**
  - rechtliche Mitgliederberatung
  - Branchenspezifische Mitgliederanfragen

- **Musterdokumente**
  - Muster AGBs
  - Mustersicherheitskonzept
  - DSGVO Code of Conduct


ispa Internet Service Providers Austria

Natalie Ségur-Cabanac

# TK Netzwerke

# Der TK Sektor als Basis für sich und andere

Natalie Ségur-Cabanac

- ✓ **Rückgrad** für unsere vernetzte Welt;
- ✓ ermöglichen **Übertragung** von Gesprächen, Daten und Multimediaanwendungen über weite Distanzen
- ✓ wesentlicher Bestandteil unseres **täglichen** Lebens, unserer Unternehmen und unserer **kritischen Infrastruktur**

# TK Netzwerke und Dienste

- **Öffentliches Telefonnetz (PSTN)**: Traditionelle analoge Telefonnetze, die Leitungsvermittlungstechnologie verwenden, um Sprachanrufe aufzubauen und aufrechtzuerhalten.
- **Mobilfunknetze**: Drahtlose Netzwerke, die Funkwellen nutzen, um mobile Geräte zu verbinden und so Sprach- und Datenkommunikation zu ermöglichen.
- **Voice over Internet Protocol (VoIP)**: Technologie, die Sprachkommunikation über das Internet ermöglicht.
- **Internet**: Ein globales Netzwerk von Netzwerken, das die Datenkommunikation unterstützt, einschließlich E-Mail, Surfen im Internet und Dateiübertragungen.
- **Private Datennetzwerke**: Netzwerke, die Organisationen gehören oder von diesen betrieben werden, für die interne Kommunikation und den Datenaustausch.

Trend zur Konvergenz/Bündelung

# Schlüsselkomponenten in TK Netzwerken

- **Knoten**: Geräte oder Punkte innerhalb des Netzwerks, die die Kommunikation ermöglichen, z. B. Telefone, Router, Switches und Server.
- **Übertragungsmedien**: physisches oder drahtloses Medium, über das Daten übertragen wird, einschließlich Kupferkabel, Glasfaser und drahtlose Funkwellen.
- **Protokolle**: Regelsätze und Standards, die die Formatierung, Übertragung und den Empfang von Daten regeln und die Interoperabilität innerhalb und zwischen Netzwerken gewährleisten.

# Funktionen von TK Netzwerken

- **Datenübertragung**: Sprache, Video und Text, zwischen Benutzern oder Geräten.
- **Signalrouting**: Netzwerke bestimmen den effizientesten Weg für die Datenübertragung.
- **Signalverstärkung**: Netzwerke verwenden Verstärker, um die Stärke von Signalen, die sich über große Entfernungen verschlechtern können, zu erhöhen.
- **Netzwerkmanagement**: Überwachung und Wartung von Netzwerkkomponenten zur Gewährleistung von Zuverlässigkeit, Sicherheit und Leistung.

# Rollen rund um TK Netzwerke

- Anbieter
- Betreiber
- Wholesale
- Endnutzer
- Benutzer

# Herausforderungen in TK Netzwerken

- **Sicherheit**: Schutz von Netzwerken vor Cyberbedrohungen, Hacking, Datenschutzverletzungen, DDoS-Angriffen etc;
- **Kapazität**: Deckung des wachsenden Bedarfs an Bandbreite aufgrund der zunehmenden Datennutzung und neuer Technologien;
- **5G**: Die Einführung von 5G-Netzwerken verspricht höhere Geschwindigkeiten, geringere Latenzzeiten und verbesserte Konnektivität für das IoT;
- **Virtualisierung**: Trend zu softwaredefinierten Netzwerken (SDN) und Netzwerkfunktionsvirtualisierung für mehr Flexibilität und Skalierbarkeit;

Natalie Ségur-Cabanac

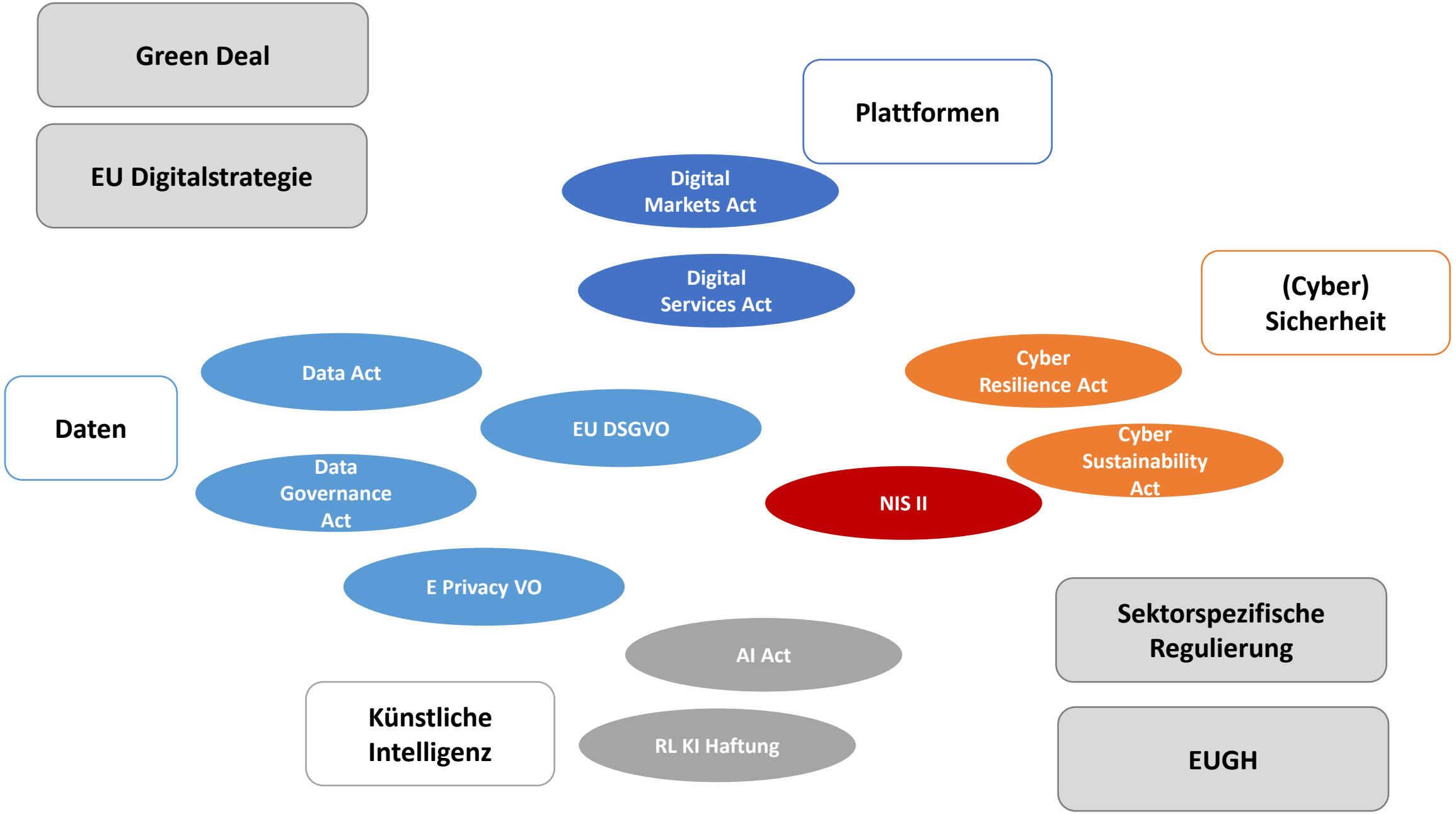
# Netzwerksicherheit

»Wer hohe Türme bauen will, muss lange am Fundament verweilen.«
(Anton Bruckner)

# Netzwerksicherheit nicht nur eine rechtliche Anforderung

- Telekommunikation ist überall
- Kritische Infrastruktur
- Datenschutz
- Regulatorische Compliance
- Reputation des Unternehmens
- Finanzielle Auswirkungen

# Regulatorisches Rahmenwerk


Green Deal
EU Digitalstrategie
Plattformen
Digital Markets Act
Digital Services Act
(Cyber) Sicherheit
Cyber Resilience Act
Daten
Data Act
EU DSGVO
Cyber Sustainability Act
Data Governance Act
NIS II
E Privacy VO
Sektorspezifische Regulierung
AI Act
Künstliche Intelligenz
RL KI Haftung
EUGH

# Rechtsrahmen EKD

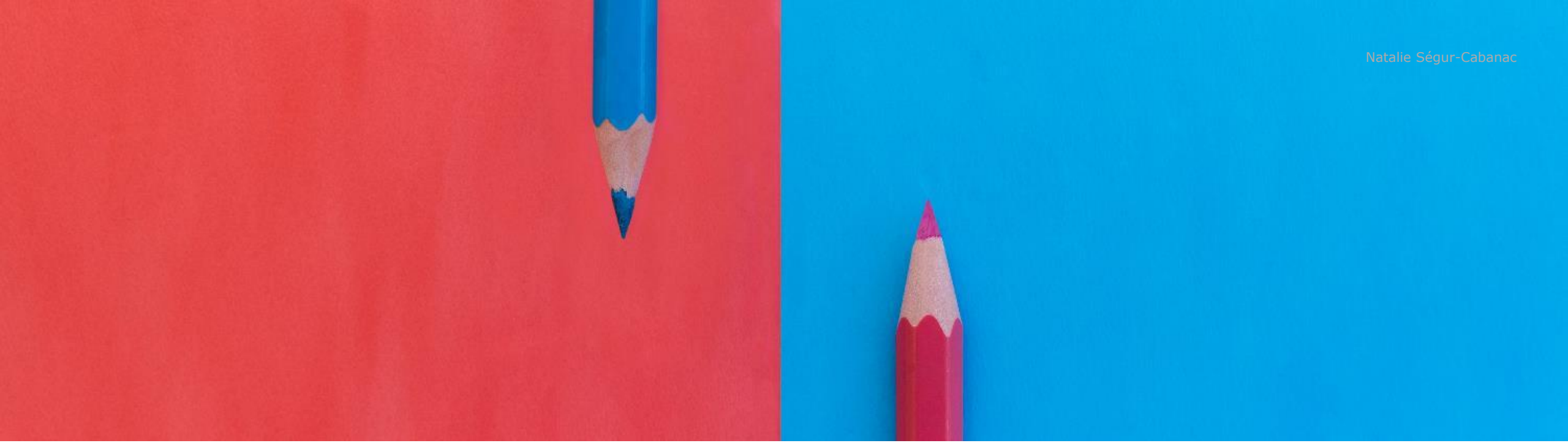
| | | | |
|---|---|---|---|
| Europ Kodex für elektron. KD | TKG 2021 | TKNIS VO | EU - 5G Security Toolbox |
| DSGVO | ePrivacy RL | NIS I | NIS II |

# Vertrag

- Vertragliche Schutz und Sorgfaltspflichten
- TK Unternehmen zu Leistungserbingung verpflichtet, schließt Sicherheit mit ein

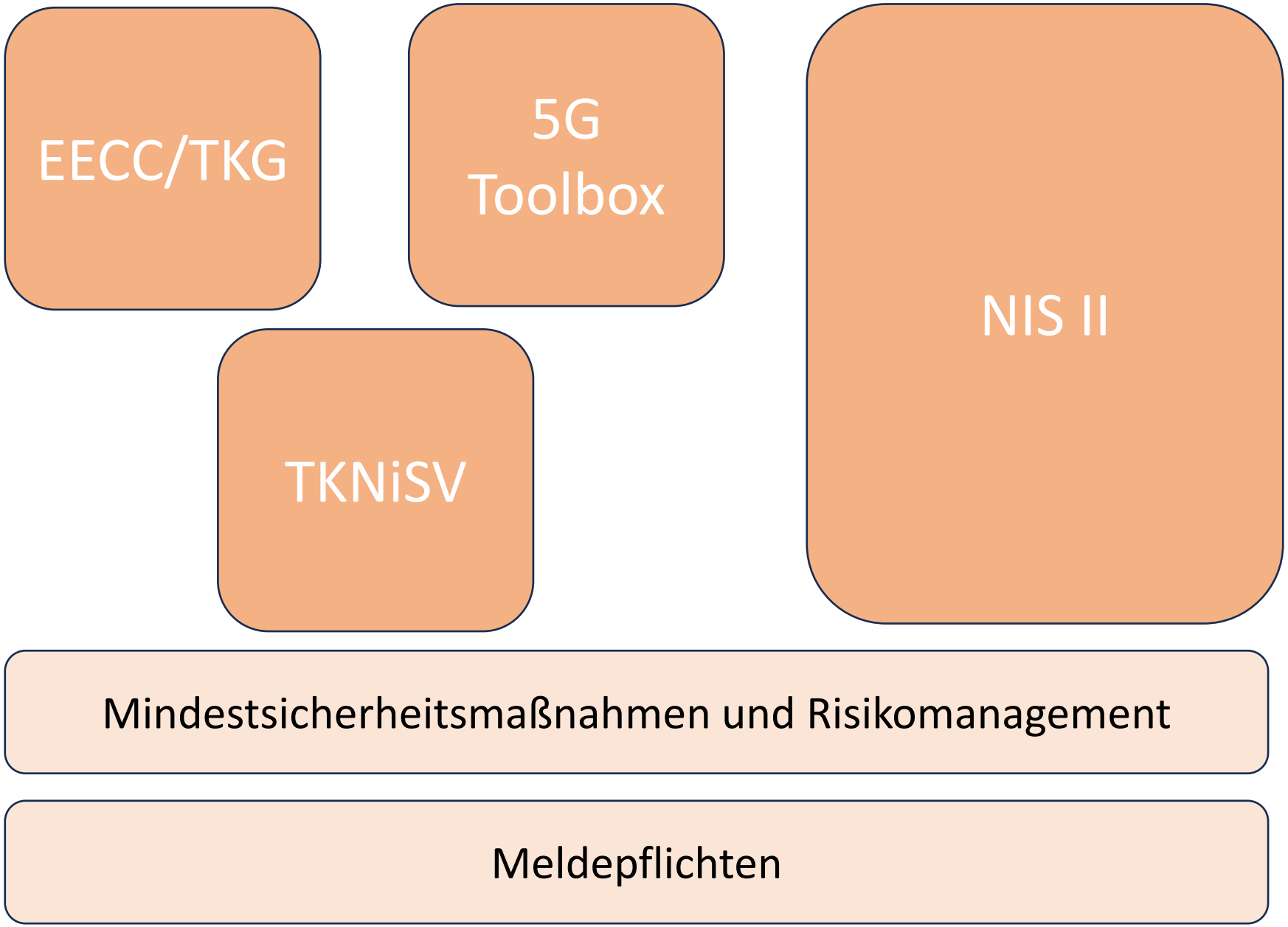
# Standards und Spezifikationen

- 3GPP
- GSMA
- ISO
- Normen
- ….



Natalie Ségur-Cabanac

# Überschneidungen und Neuerungen.


EECC/TKG
5G Toolbox
NIS II
TKNiSV
Mindestsicherheitsmaßnahmen und Risikomanagement
Meldepflichten

# Risikomanagementmaßnahmen allgemein

| EECC/TKG | 5G-Toolbox/TKNiSV | NIS II |
|---|---|---|
| § 44 (1) TKG<br><br>**Sicherheit und Integrität** von **Netzen** | § 5 TKNiSV<br><br>• Risikomanagement<br>• Betriebliches Kontinuitätsmanagement<br>• Störfallmanagement<br>• Fortlaufendes Monitoring | Art 21 Abs 2<br><br>• Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;<br>• Bewältigung von Sicherheitsvorfällen<br>• Aufrechterhaltung des Betriebs |

# Risikomanagementmaßnahmen (Lieferkette)



| EECC/TKG | 5G-Toolbox | TKNiSV | NIS II | Δ |
|---|---|---|---|---|
| **§ 45 TKG High Risk Supplier** | **High Risk Supplier**<br><br>Forcierung von **Multi-Vendor-Strategien** um die Abhängigkeit von einem Hersteller zu reduzieren<br><br>Verbesserung der Sicherheit im **Bestell-Prozess** | **Multi-Vendor-Strategie**, die die technischen Beschränkungen und Interoperabilitäts-anforderungen verschiedener Teile eines **5G-Netzes** berücksichtigt. (§ 6) | **Sicherheit der Lieferkette** einschließlich **sicherheitsbezogene r** Aspekte der **Beziehungen** zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern; (Art 21) | § 6 TKNSiV gilt **nur** für Sicherheitsanforderungen an **5G-Netze**<br><br>§ 45 TKG 2021 **Hochrisikolieferanten**<br><br>Laut NIS II soll **Cybersicherheit** in **Verträge** aufgenommen werden.<br><br>Siehe auch **Cyber Resilience Act** (physische Sicherheit) |

# Berichtspflichten

| EECC/TKG | 5G-Toolbox | TKNSiV | NIS II | Δ |
|---|---|---|---|---|
| § 44 (5) TKG **Meldepflichten** von Sicherheitsvorfällen | - | Erheblicher Sicherheitsvorfall bestimmt sich **nach Anzahl der Teilnehmer** (§ 3 Abs 2).<br><br>Unverzügliche Meldung ab Kenntnis des Sicherheitsvorfalls sowie innerhalb von 24h eine umfassende Informationen zum Sicherheitsvorfall. | Ein Sicherheitsvorfall gilt als **erheblich**, wenn a) er **schwerwiegende Betriebsstörungen** der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen **kann**; b) er **andere** natürliche oder juristische **Personen** durch **erhebliche materielle** oder **immaterielle** Schäden **beeinträchtigt** hat oder beeinträchtigen **kann** (Art 23). | NIS II **nicht** bloß an **Schwellenwerten** orientiert.<br><br>Zuständigkeiten sind noch nicht geklärt.<br><br>NIS II Unverzügliche Meldung bzw. spätestens innerhalb von 24h Frühwarnung, umfassende Meldung erst innerhalb von 72h, Abschlussbericht nach einem Monat. |

# Aufsicht

| EECC/TKG | 5G-Toolbox | TKNSiV | NIS II | Δ |
|---|---|---|---|---|
| RTR | Durchführung von **Sicherheits-Audits** bei Betreibern | Monitoring, Audits, Tests (Monitoring/Protokollierung, Stellvertretungs- und **Notfallsübungen**, **Systemtests**, Sicherheitsbewertung, **Konformitätsüberwachung** und **Auditierungsverfahren**). (§ 5) | **Aufsicht für wesentliche Einrichtungen**<br>▪ Vor-Ort-Kontrollen<br>▪ gezielte Sicherheitsprüfungen<br>▪ Ad-hoc-Prüfungen<br>▪ Sicherheitsscans<br>▪ Anforderung von Informationen<br>▪ Anforderung von Nachweisen für die Umsetzung der Cybersicherheits-konzepte<br>(Art 32) | **Ad hoc – Kontrolle für wesentliche Einrichtungen**. |

# Zertifizierungen

| EECC/TKG | 5G-Toolbox | TKNSiV | NIS II | Δ |
|---|---|---|---|---|
| - | **EU-weite Zertifizierung – Vorläufig über Konformitätserklärung** abgedeckt;<br>▪ EU-Zertifizierung für **5G Netzkomponenten, Kundenequipment** und **Prozesse** bei Herstellern<br>▪ EU-Zertifizierung für weitere **Non-5G Komponenten** und Dienste (wie **connected devices** und **cloud services**) | - | Die Mitgliedstaaten können die Unternehmen dazu verpflichten, nur **bestimmte ICT Produkte oder Dienste** zu verwenden, die ein europäisches **Cybersicherheitszertifikat** erhalten haben. | Zertifizierung möglich, es bedarf noch Ausführungsgesetzgebung |
| | | | **Delegierte Rechtakte der EK. (Art 24)** | |

# Governance

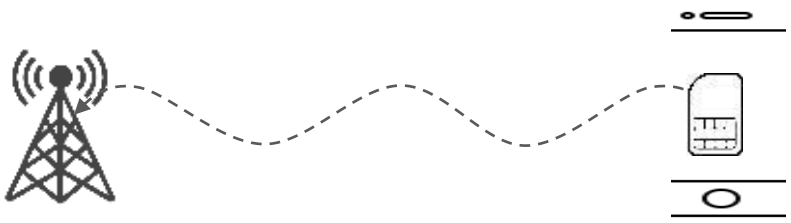
| EECC/TKG | 5G-Toolbox | TKNSiV | NIS II | Δ |
|---|---|---|---|---|
| | | | **Leitungsorgan muss primär die notwendigen Organisationsschritte** setzen, deren Implementierung **sicherstellen** und laufend **kontrollieren** (lassen) und die Umsetzung laufend **verbessern** (wenn sich Verbesserungsbedarf ergibt | **Leitungsorgane**<br><br>(Haftung Geschäftsführung, z. B. 22 Abs 1 GmbHG) |
| | | | **Leitungsorgane** haben an **Schulungen teilzunehmen** (Art 20). | Schulungen |

# Bedrohungen von TK Netzen

# Netzabschlusspunkt

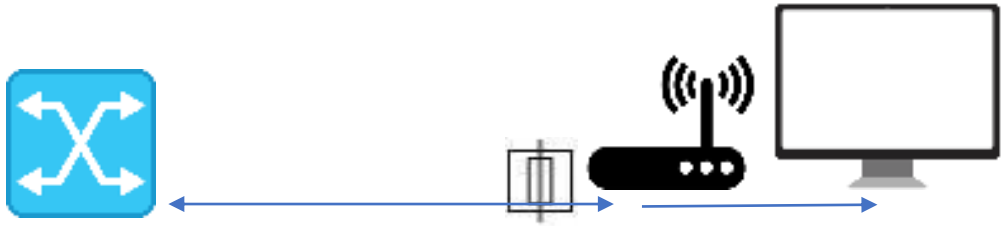
Mobilnetz

Öffentliches mobiles Kommunikationsnetz in Ö.



Feste Breitbandnetze

Öffentliches festes Kommunikationsnetz in Ö.



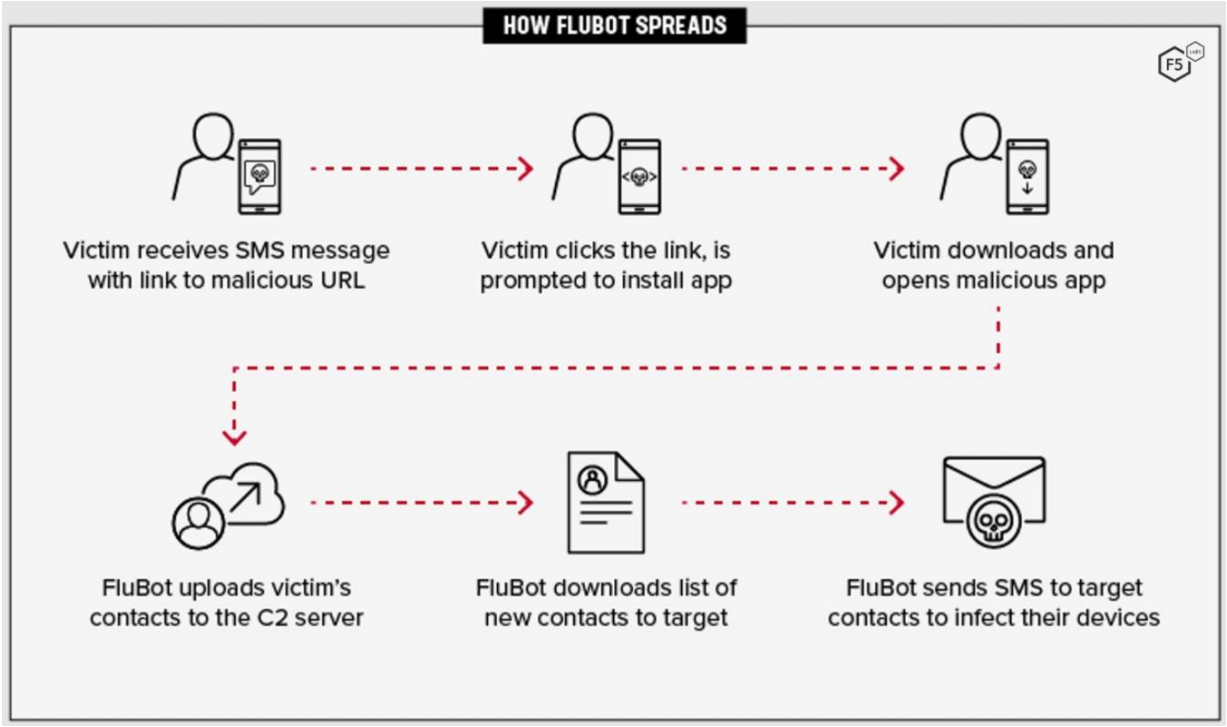
TKG 2021

- der **physische** Punkt,
- an dem einem **Endnutzer** der **Zugang** zu einem **öffentlichen** Kommunikationsnetz **bereitgestellt** wird,
- und der in Netzen, in denen eine **Vermittlung** oder **Leitwegbestimmung** erfolgt, anhand einer bestimmten **Netzadresse** bezeichnet wird, die mit der **Nummer** oder dem **Namen** eines Endnutzers **verknüpft** sein kann.

# SMS Betrug via Flubot Virus


Natalie Ségur-Cabanac

- SMS von angeblichen Paketlieferdiensten mit Nachrichten wie „Die gekaufte Ware wurde versendet“, „Ihr Paket wurde verschickt“;
- Ziel: Der Empfänger soll auf den mitgesendeten Link klicken, wodurch eine Malware in Form einer bösartigen App am Gerät installiert wird;
- Schadsoftware verschickt über die betroffene Rufnummer Massen-SMS, u.a. an die am Smartphone gespeicherten Kontakte sowie ins Ausland, was zu erheblichen Kosten führen kann.
- SMS scheint in der Versandübersicht nicht auf; Schadsoftware verbreitet sich über SMS rasant weiter;
- Wahres Ziel: Bankinformationen vom Opfer zu stehlen;
- Vorwiegend Andorid Betriebssystem betroffen;




**FluBot spread process diagram**
*Source: F5 Labs*

# SMS Betrug via SIM Swap

- Kriminelle sammeln Informationen über ihre Opfer via Online Recherchen, Phishing, sozialen Netzwerken, Data Leaks, Social Engineering etc;
- Mit den gesammelten Daten gibt sich Betrüger beim MF Anbieter als Opfer aus und bewirkt Ersatz SIM Karte;
- Betrüger erhält Anrufe/SMS inklusive SMS TAN von Banken;

# Angriffe auf Systeme von außen

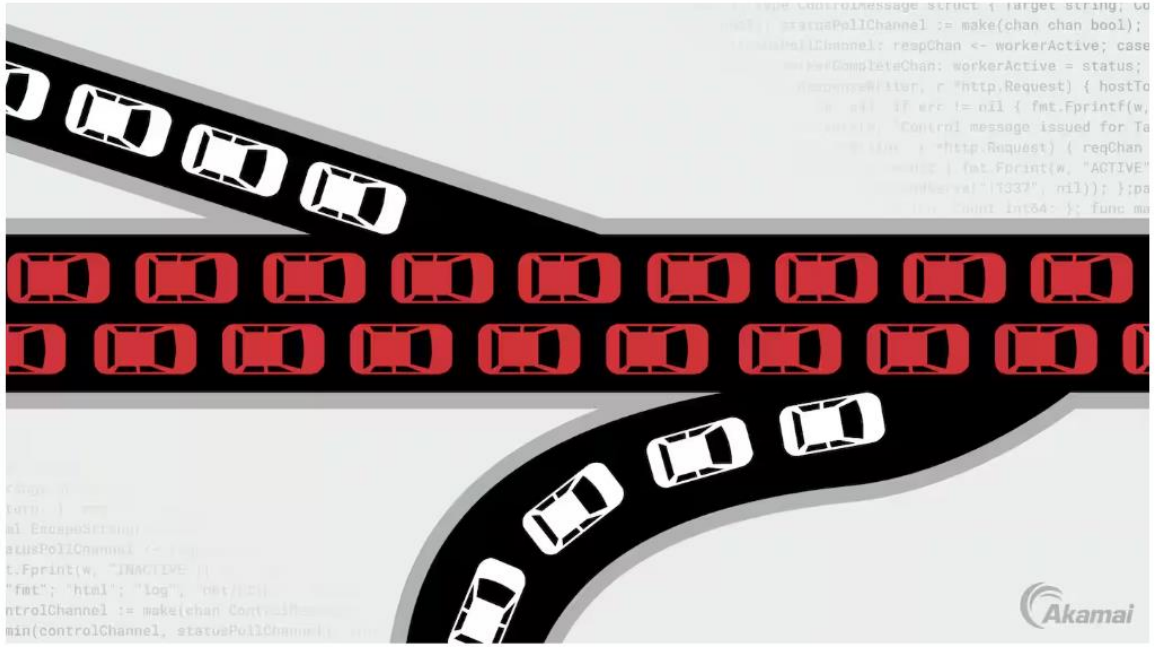
## DDoS Attacken

Angreifer überfordert sein Ziel mit unerwünschtem Internettraffic

=> normaler Traffic erreicht das vorgesehene Ziel nicht.

=> „Verkehrsstau“, kein traffic kommt mehr durch

=> Ausfall von Systemen und Nichtverfügbarkeit von Diensten



# Angriff auf physische Infrastruktur

Handelsblatt

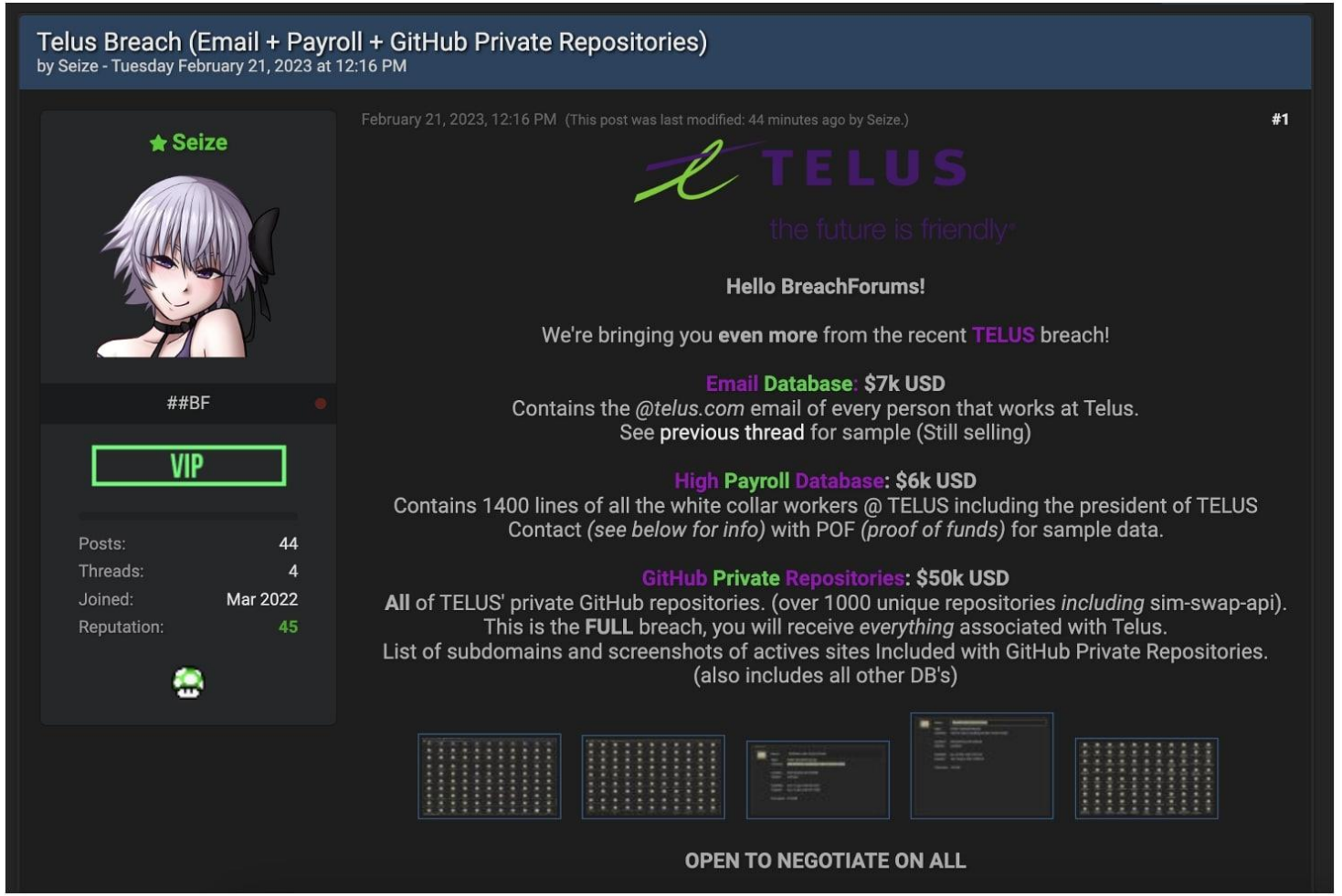
Coronavirus

## Verschwörungstheorien motivieren zu Anschlägen auf 5G-Masten

In Europa kommt es vermehrt zu Anschlägen auf 5G-Masten. Grund dafür sind Verschwörungstheorien, die Mobilfunkstrahlung für die Corona-Pandemie verantwortlich machen.

Stephan Scheuer
24.04.2020 - 17:05 Uhr

# Falsche Konfiguration von Systemen



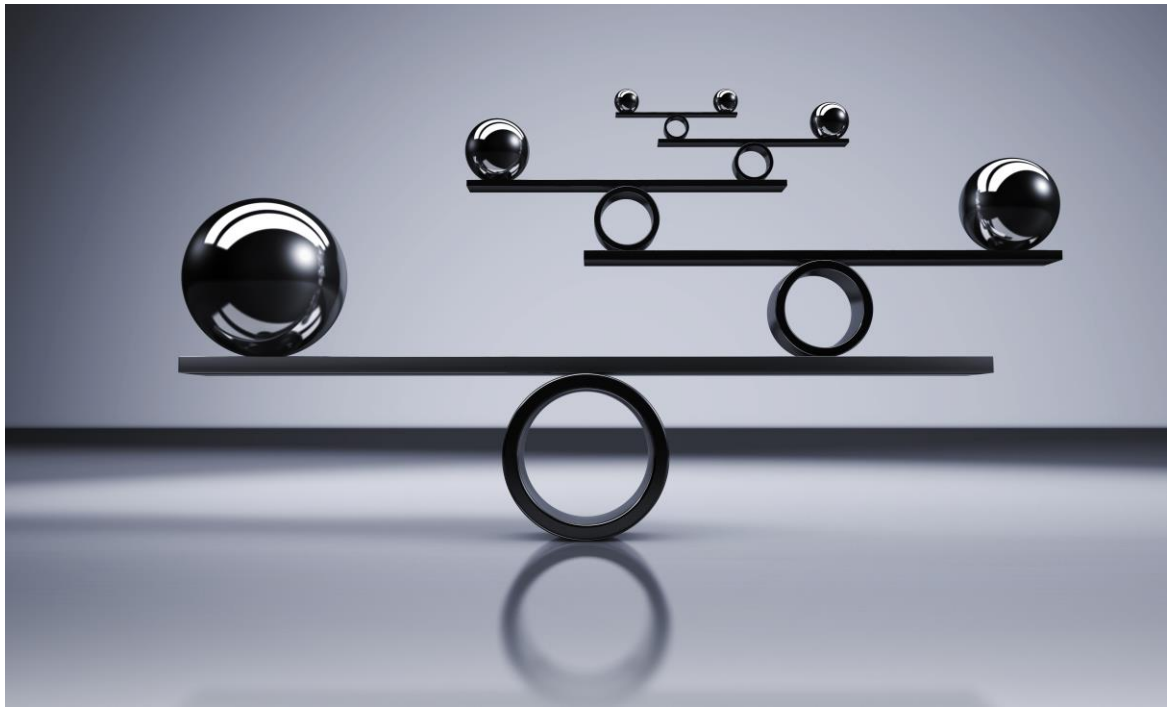

## 2021 Telus Kanada Data Breach

- Miskonfiguration bei einem Auftragsnehmer von Telus
- Daten von Telus Kunden wurden offen gelegt


# Datensicherheitsverletzungen/Data Breaches

Personenbezogene Daten (Kunden, Mitarbeiter, Lieferanten) werden zweckwidrig verarbeitet, offengelegt, gehen verloren oder werden zerstört

# Verantwortlichkeit geht über Grenzen



## Over 5,000 Wind Tre customers hit by data breach

Posted on June 9, 2017 by Dissent

Telecompaper reports:

> Italy's data protection authority, Garante Privacy, has ordered **Wind Tre** to write to customers to notify them of a data breach that occurred on 20 March. Tech website Key4Biz reports that some 5,118 customers may have been affected when the service provider responsible for the Self Care 3 area was attacked. A total of 402 of the 5,118 customers could also have been victims of unauthorised access to their personal data including user ID and login credentials.

Read more on Telecompaper.

https://www.databreaches.net/over-5000-wind-tre-customers-hit-by-data-breach/

# Ganz konkret

# Best Practices

- Risikoassessment
- Mitarbeiter Schulungen und Awareness
- Zugangs- und Zugriffskontrolle UND Protokollierung
- Strenge Passwörter, Multi-Factor Authentication
- Verschlüsselung
  - Achtung auf nationale Verbote von Verschlüsselung, zB bei Roaming)
  - Daten in Ruhe und bei Übertragung
- Regelmäßige Updates und Patch Management

# Best Practices /2

- Netzwerk Monitoring and Intrusion Detection
- Network Segmentation
- Lieferanten Sicherheitsbewertung
- Incident Response Plan
- Sicherheits Audits and Penetration Tests
- Compliance with Industry Standards (e.g., NIST, ISO 27001)
- Compliancemanagementsytem: Prevent- Detect – React
- Datenschutzmanagementsystem – data privacy by design

# Dr. Natalie Ségur-Cabanac

natalie.segur-cabanac@ispa.at