Netzsicherheit im Spannungsfeld von Politik und Technik

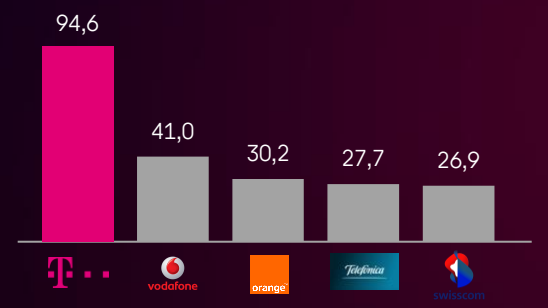
Wolfgang Kopf, Salzburg, 5. September 2022

LIFE IS FOR SHARING.

Deutsche Telekom auf einen Blick

01 Größte europäische Telco

Marktkapitalisierung (Mrd. €)



Updated 29.06.2022

02 Stark in Europa

Mobilfunkkunden

101 Mio.

Breitbandanschlüsse

30 Mio.

Kunden in Europa, Stand 30.06.2022. Breitbandanschlüsse: Summe Retail und Wholesale.

03 Führend bei Netzqualität & Kundenzufriedenheit

(Alle)

We win awards

Beste Netze

Beste Produkte

Bester Service

04 Überdurchschnittlich bei Netz-Investitionen

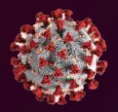
Investitionen 2021 weltweit

18 Mrd. Euro

+5,9% im Vergleich zum Vorjahr

Ohne Ausgaben für Mobilfunkspektrum

05 Verlässlich in Krisenzeiten



Stabile Netze in Zeiten massiver Verkehrssteigerungen

Corona-Warn-App von DT und SAP (46,8 Mio. Downloads)

Schnelle Hilfe vor Ort und Wiederherstellung der Kommunikationsnetze

06 Telekom Security: Best-in-Class

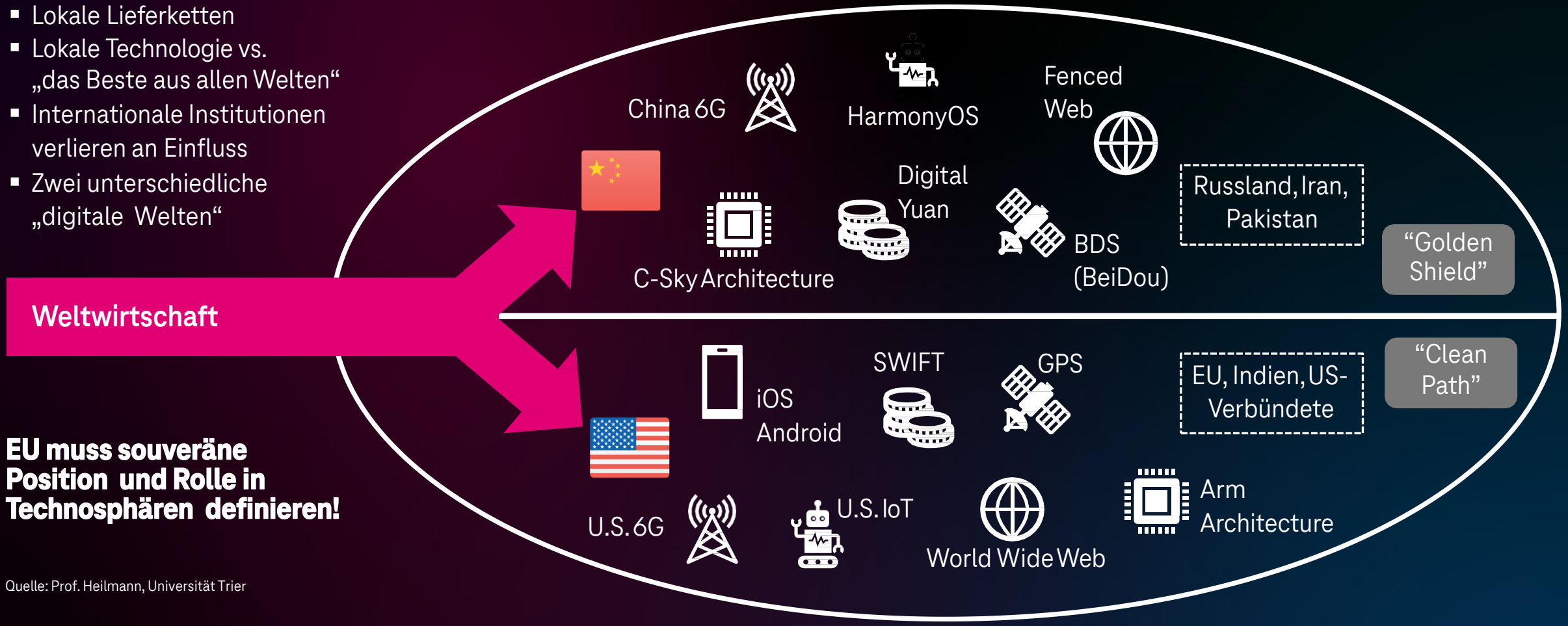
> 1.600 Experten
Vollständiges Sicherheitsportfolio
Investitionen € 250 Mio. p.a.

Sichert DT und externe Kunden mit Security Operations Center 24/7 ab; enge Kooperation mit Sicherheitsbehörden in EU

Marktführer in D; führende internationale Partner und Kooperationen

„Digitaler Eiserner Vorhang“: Zwei Technosphären

- Lokale Lieferketten
- Lokale Technologie vs. „das Beste aus allen Welten“
- Internationale Institutionen verlieren an Einfluss
- Zwei unterschiedliche „digitale Welten“



EU muss souveräne Position und Rolle in Technosphären definieren!

Quelle: Prof. Heilmann, Universität Trier

Geopolitische Entwicklungen und Klimawandel führen global zu steigenden Risiken – Naturkatastrophen, Extremwetter, Cyberangriffe

Finanzmarkt-volatilität

Humanitäre Krisen

Energie-engpässe

- Folge: Notwendigkeit zu beschleunigter Diversifizierung, erhöhte Unabhängigkeit und Redundanz

- Folge: Suche nach Alternativen, verstärkte Diversifizierung und Bevorratung

Lieferketten unter Druck

Rohstoff-knappheit

Divergierende Technologie-standards

- Folge: Verstärkter Trend zur Entwicklung separater Standards und unabhängiger digitaler Technologien

- Folge: Notwendigkeit zur Erhöhung von Resilienz und Reaktionsfähigkeit, Verbesserung von Warnsystemen

Natur-katastrophen

Höhere Verteidigungs-ausgaben

Drohende Cyberangriffe

- Folge: Permanente Verbesserung der Cybersicherheit (Vorbeugung und Abwehr) erforderlich

Öffentlicher Katastrophenschutz in Europa seit Anfang der 90er Jahre vernachlässigt!

Handlungsfelder bezüglich Telekommunikation

RESILIENZ

WEITESTMÖGLICHE WIDERSTANDSFÄHIGKEIT GEGEN ADVERSE EINFLÜSSE

ABER: Öffentliche Netze sind in erster Linie für den Alltag vorgesehen und sind heute nicht primär als Kommunikationsmittel für Katastrophenfälle konzipiert

Ausgewählte Bedrohungsszenarien (RTR und BNetzA)

- **Ausfall / Mangellage bzgl. Betriebsmitteln, insbesondere Strom**
- **Naturkatastrophen, außergewöhnliche klimatische Bedingungen**
- **Cyberkriminalität**
- Vorsätzliche Beschädigung, Manipulation, Zerstörung, Sabotage, Diebstahl
- Vertraulichkeitsverlust von geschützten Informationen, Spionage
- Ausfall von zentralen nationalen Internet-Exchanges
- Ausfall oder erhebliche Serviceeinschränkungen bei/von singulären IKT-Lieferanten
- Verwundbarkeiten bei Hard- und Software
- Mängel in der Betriebsführung, mangelhaftes Notfall-, Krisen- und Kontinuitäts-Management, Defizite im Beschaffungsprozess
- Kriegerische Auseinandersetzungen, ..., elektromagnetischer Puls (nuklear und nichtnuklear)

Resilienzmaßnahmen – Best Practice in 3 Phasen

1 PREPARATION: VORBEUGUNG + FÄHIGKEITEN

- **Priorisierung kritischer Infrastrukturen inkl. Mobilfunk (Vorrang bei Zugang, Transport, Kraftstoff)**
- Vulnerability Management: Sichere Konfiguration und Updates
- Detaillierte Notfallpläne
- Redundante Netzanbindungen
- Einrichtung gemeinsames Lagezentrum von KritIS-Netzbetreibern und Behörden
- Warnsysteme (z.B. Cell Broadcasting, Sirenen)
- Ersatzsysteme (z.B. mobile Mobilfunkstationen, Generatoren)
- **Maßnahmen sollten angemessen sein und durch bestgeeigneten Akteur erfolgen** (z.B. gegen Stromausfälle primär durch Stromversorger)

2 INCIDENT HANDLING

3 RECOVERY

PERMANENTE AKTUALISIERUNGEN UND NOTFALLORGANISATION MIT REGELMÄßIGEN ÜBUNGEN ALLER AKTEURE

Resilienzmaßnahmen – Best Practice in 3 Phasen

1 PREPARATION

2 HANDLING: WÄHREND VORFALL & UNMITTELBAR

Vorbereitet im Krisenfall

- Klare Verantwortung in effektivem Krisenstab
- Kurze Entscheidungswege
- Entschlossenheit
- Flexibilität

„Faster is better than perfect“!

3 RECOVERY

PERMANENTE AKTUALISIERUNGEN UND NOTFALLORGANISATION MIT REGELMÄßIGEN ÜBUNGEN ALLER AKTEURE

Resilienzmaßnahmen – Best Practice in 3 Phasen

1 PREPARATION

2 INCIDENT HANDLING

3 RECOVERY: WIEDERHERSTELLUNG UND VERBESSERUNG

- **Ausführung der Backup-Wiederherstellungskonzepte**
- **Überbrückungslösungen** bei längerer Wiederherstellungs-dauer
- **Wiederaufbau** wo möglich mit moderneren und resilienteren Technologien und an besser geeigneten Standorten

PERMANENTE AKTUALISIERUNGEN UND NOTFALLORGANISATION MIT REGELMÄßIGEN ÜBUNGEN ALLER AKTEURE

Sommerflut Juli 2021
Am stärksten betroffene Gebiete

Telekommunikationsinfrastruktur umfassend zerstört oder beschädigt

304 Mobilfunkstandorte gestört (Stromversorgung, Hardware, Anbindung)

250.000 Menschen ohne Mobilfunk

Backbone und Anbindung massiv betroffen, 3 Hauptknoten vollständig zerstört

102.000 Festnetzanschlüsse defekt

Bsp. Altenahr / Ahrtal

Handling & Recovery: Telekom mit umfangreicher und schneller Hilfe

ERSTE NOTFALLMASSNAHMEN

Lagebild und Aktivierung Schnelleinsatzteam

HIGHLIGHTS

- **Aufbau mobiler Mobilfunkstationen, temporäre Backbone-Anbindung, Vermittlungsstellen in Containern**
- “Rucksack-Teams”: Verteilung > 5,000 Mobiltelefone plus Power Banks
- Rechnungen und “Mahnsperren” für alle betroffenen Kunden gestoppt
- Unlimited-Tarife für Kunden und Helfer

SCHNELLE HILFE FÜR BETROFFENE

Konzentration auf die Bürger

HIGHLIGHTS

- **80% Recovery des Mobilfunknetzes nach 3 Tagen, 99% nach zwei Wochen**
- Betreuung von 62.100 Kunden vor Ort, Reparaturquote >90%
- Mobile Service Points für >4 Monate vor Ort
- **Übergangsprodukte für alle betroffenen Festnetzkunden (12 Monate kostenlos)**
- 2.000 Mitarbeiter unterstützten freiwillig

LÄNGERFRISTIGER WIEDERAUFBAU

Bau eines stärkeren Netzes als vorher

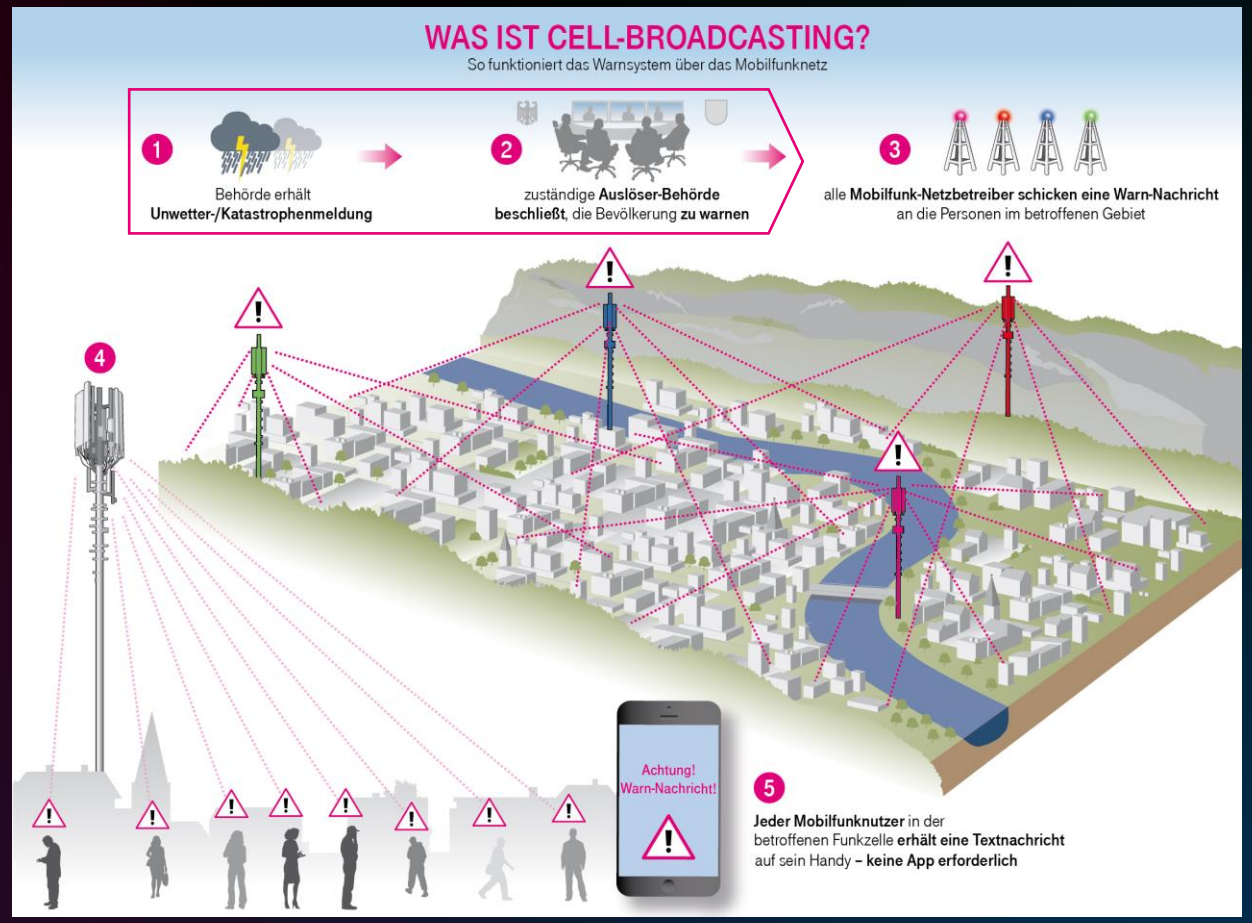
HIGHLIGHTS

- 96% alle Festnetzverbindungen wieder-hergestellt
- **Neubau von 35.000 Glasfaseranschlüssen**
- **FTTH “Spatenstiche” nach höchstens 6 Monaten**
- Normalbetrieb des Rechnungsverfahrens zuletzt

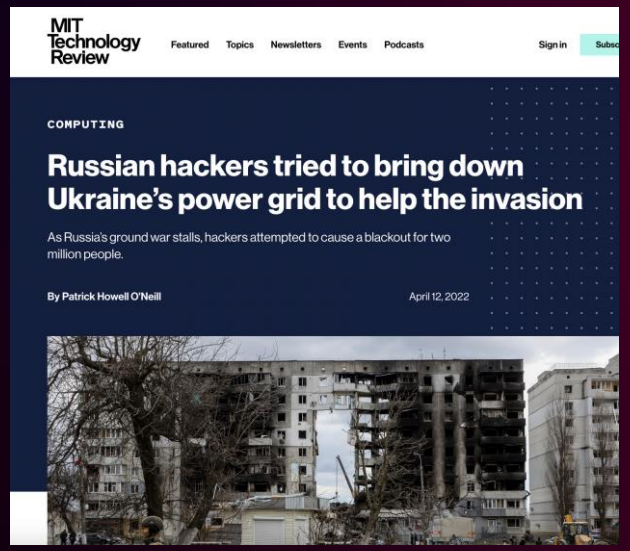
INTENSIVE ZUSAMMENAREIT ZWISCHEN BNETZA, NETZBETREIBERN, LOKALEN BEHÖRDEN UND HILFSORGANISATIONEN

Öffentliche Warnungen: Cell Broadcasting, Verzahnung mit anderen Informationskanälen und behördlichem Warnsystem

- **Cell Broadcasting ist schnell, effektiv, international bewährt** (SMS zu langsam, Apps weniger verbreitet)
- Österreich verfügt über Warn-App und SMS-basierte Lösung, in Deutschland wird Cell Broadcasting gerade (wieder) eingeführt.
- **Das Warnsystem** sollte auf **umfassender Warn- und Informationsstrategie basieren & eng verzahnt umfassen**:
  - Sirenen und Lautsprecher,
  - Rundfunk,
  - Einsatzkräfte,
  - etc.
- **Auch notwendig: Integration aller Informationskanäle in strukturiertes behördliches Warnsystem**
  mit klar definierten Prozessen, Rollen und Rechten
  (in DE z.B. behördliches **Modulares Warnsystem (MoWaS))**



Stromengpässe oder Cyberangriffe: Funktionstüchtige und resiliente Stromnetze gefordert


MIT Technology Review
Featured Topics Newsletters Events Podcasts Sign in

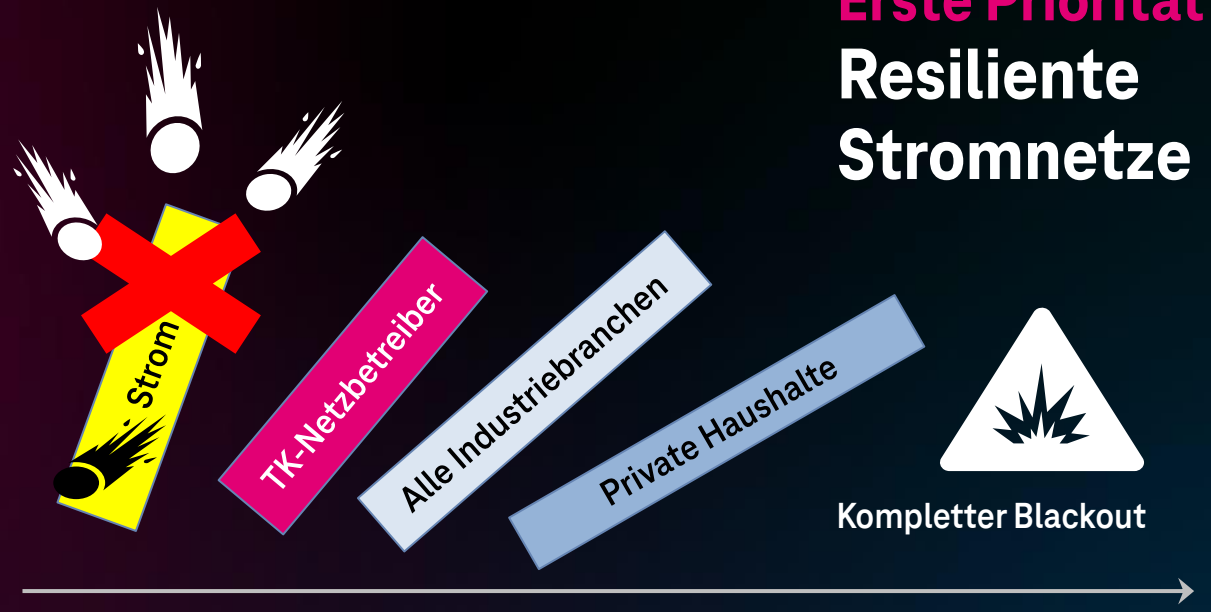
COMPUTING

Russian hackers tried to bring down Ukraine's power grid to help the invasion

As Russia's ground war stalls, hackers attempted to cause a blackout for two million people.

By Patrick Howell O'Neill April 12, 2022

Fallbeispiel: gezielter Cyberangriff auf das Stromnetz der Ukraine



Erste Priorität
Resiliente Stromnetze

Abhilfe gegen Stromengpässe bzw. -ausfälle

- Energieversorger: Resilienzerhöhung und Priorisierung kritischer Infrastruktur
- Notstromversorgung Mobilfunk (immenser Aufwand, sehr langwieriger Aufbau, geringe Akzeptanz)
- Tbd: Basisversorgung Mobilfunk (weniger Strombedarf, aber auch Leistungsfähigkeit eingeschränkt)
- Alternativnetze (Satelliten) und -Endgeräte als Fallback
- Kundenseitige Maßnahmen (z.B. Power Banks)

CYBERSECURITY

"THE COLLECTION OF TOOLS, POLICIES, SECURITY CONCEPTS, SECURITY SAFEGUARDS, GUIDELINES, RISK MANAGEMENT APPROACHES, ACTIONS, TRAINING, BEST PRACTICES, ASSURANCE AND TECHNOLOGIES THAT CAN BE USED TO PROTECT THE CYBER ENVIRONMENT AND ORGANIZATION AND USERS' ASSETS."
(ITU 2008)

Cybersecurity: Immer mehr Ziele und Angreifer

Cybersecurity in Zahlen

26% pro Jahr

Cybercrime wachsend in Österreich

(Bundesministerium des Innern, 3/2021)

$ 265 Milliarden

Globaler Schaden allein durch Ransomware bis 2031

Andere Angriffsarten dabei noch gar nicht berücksichtigt
(Cybersecurity Ventures, 6/2022)

€ 203 Milliarden

Schaden p.a. durch Angriffe auf deutsche Unternehmen

9 von 10 Unternehmen Opfer von Datendiebstahl, Spionage, Sabotage; Angriffe aus Russland und China sprunghaft angestiegen
(Bitkom 8/2022)

10%

der betroffenen Kleinunternehmen mussten schließen

Nicht alle Unternehmen überleben eine Attacke (lt. Allianz für Cyber-Sicherheit)

DT-Lagebild Cybersecurity – KPIs Juli 2022

53.0 Mio. Angriffe
pro Tag gegen DT-Honeypot-Infrastruktur; historisch höchster Wert = >90 Mio. Angriffe pro Tag

1.762
Botnet-Server identifiziert und geblockt

362
Botnet-infizierte Kunden im Wochendurchschnitt geschützt

87.7 Gbit/s
Angriffskapazität der größten DDoS Attacke

110.618
Missbrauchshinweise an Kunden verschickt

Echtzeit-Lagebild zu Angriffen auf DT-Honeypots:
www.sicherheitstacho.eu

Unsere Antwort: T-Sec & Security Operations Center (SOC)

- **> 1.600 Experten insgesamt**, Marktführer in D, mehr als 140 österreichische Behörden & Unternehmen als Kunden.
- SOCs sind die **Cyber-Abwehrzentralen der Telekom. Das SOC-Netzwerk** hat neben dem **„Master-SOC“ in Bonn** weitere Standorte im DACH-Verbund (**Österreich**), sowie sechs lokale SOCs weltweit (Ungarn, Tschechien, Spanien, Brasilien, Mexiko und Singapur).
- **200 Security-Spezialisten** beobachten 24/7 die "Bedrohungsland-schaft" in den Netzen:
  - **Threat Intelligence Team** (TI) -> Analyse, Forensik
  - **Abuse Team** -> Hilfe für angegriffene Kunden
  - **Computer Emergency Response Team** (CERT) -> Kooperation mit staatlichen Stellen / Sicherheitsbehörden
  - **Red Team** -> „Interne Hacker“; melden gefundene Schwachstellen

Angriffe werden in Echtzeit erkannt, abgewehrt und analysiert!

Vielen Dank!