Datenaustausch und Kommunikation

Gesicherte Kommunikation im Krisenfall

Szenarien/Maßnahmen

Graz 02.10.2024

Dipl.Ing (HTL) Leopold K

Latente Bedrohungsszenarien:

Stromausfall
Netzwerk – IT Crash
- Cybercrime, Virenattacken, Denial of Service
Vandalismus
Bombendrohung
Brand
Erdbeben, Erdrutsch, Muren, Überschwemmung
Pandemie

Worst Case: Black Out

- Bei längem Stromversorgungsausfall ist nach nur 30 Minuten keine ausreichende Kommunikation sowohl über Festnetz- und Mobilfunknetz möglich
- Sprachtelefonie, Datenübertragung, Zugang ins Internet und zu Daten die in Cloudservern gehosted sind, sind nicht mehr verfügbar.
- BOS- Funk wird von Blaulichtorganisationen verwendet und steht nicht für die notwendige interne Kommunikation ausreichend zur Verfügung
- Funknetze alleine reichen nicht- mangelnde Störsicherheit, nicht abhörsicher, Witterungsabhängigkeit

Abhängigkeiten Umwelt/Technologie

- **Energiewende**

  - Auswirkung auf nationale & Internationale Stromverteilerinfrastruktur (Umstieg auf Wind und Solarenergie)
  - Stromüberschuß privater Abnehmer muss in öffentliche Netze abgeführt und verteilt werden

- **Technologiewandel/Digitalisierung- Fluch und Segen**

  - Totale Abhängigkeit von Public Internet & Cloudlösungen
  - Totale Abhängigkeit von der Verfügbarkeit der Stromversorgung
  - Cyber Kriminalität
  - Delay der Sicherheitsmaßnahmen zum technologischen Fortschritt

- **Künstliche Intelligenz**

- **Weichenstellungen und Maßnahmen der öffentlichen Hand notwendig**

  - Erste Ansätze NIS1/2 und RKE im Prozessialen Umfeld vorhanden - Gesamtlösung für gesicherte Krisenkommunikation fehlt

Wie sicher ist die Telekommunikationsinfrastruktur Österreichs?

Ist die Republik Österreich, ihre Einsatzorganisationen und die Wirtschaft/Unternehmen in Österreich darauf vorbereitet, die Kommunikation und damit die Handlungsfähigkeit sicher zu stellen

?

Gesetzliche Verantwortlichkeiten und Rahmenbedingunge

ITSPreventexpert

Bundeskanzleramt

Bundesministerium
Landesverteidigung

Bundesministerium
Arbeit und Wirtschaft

Bundesministerium
Inneres

Bundesministerium
Klimaschutz, Umwelt,
Energie, Mobilität,
Innovation und Technologie

Bundesministerium
Bildung, Wissenschaft
und Forschung

Bundesministerium
Europäische und internationale
Angelegenheiten

§

Risikoanalyse SKI

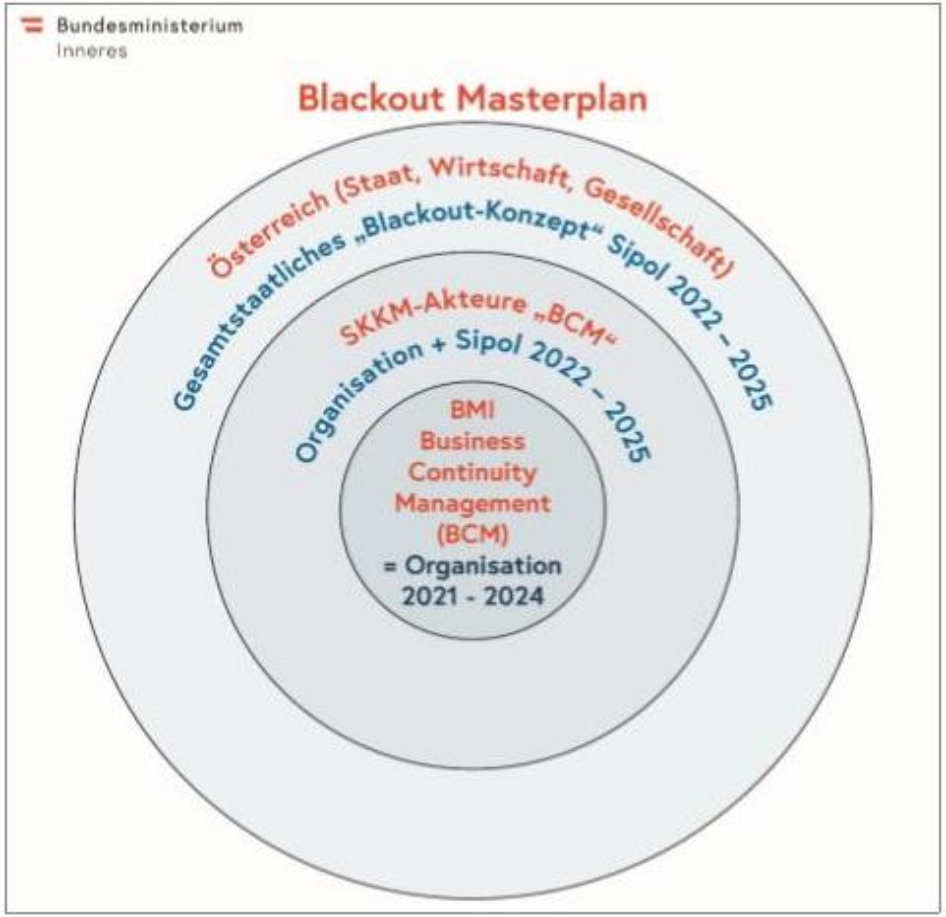
NIS/ RKE

Datenschutzgrundverordnung

Verbandsverantwortlichkeitsgesetz VbVG

Black Out Masterplan

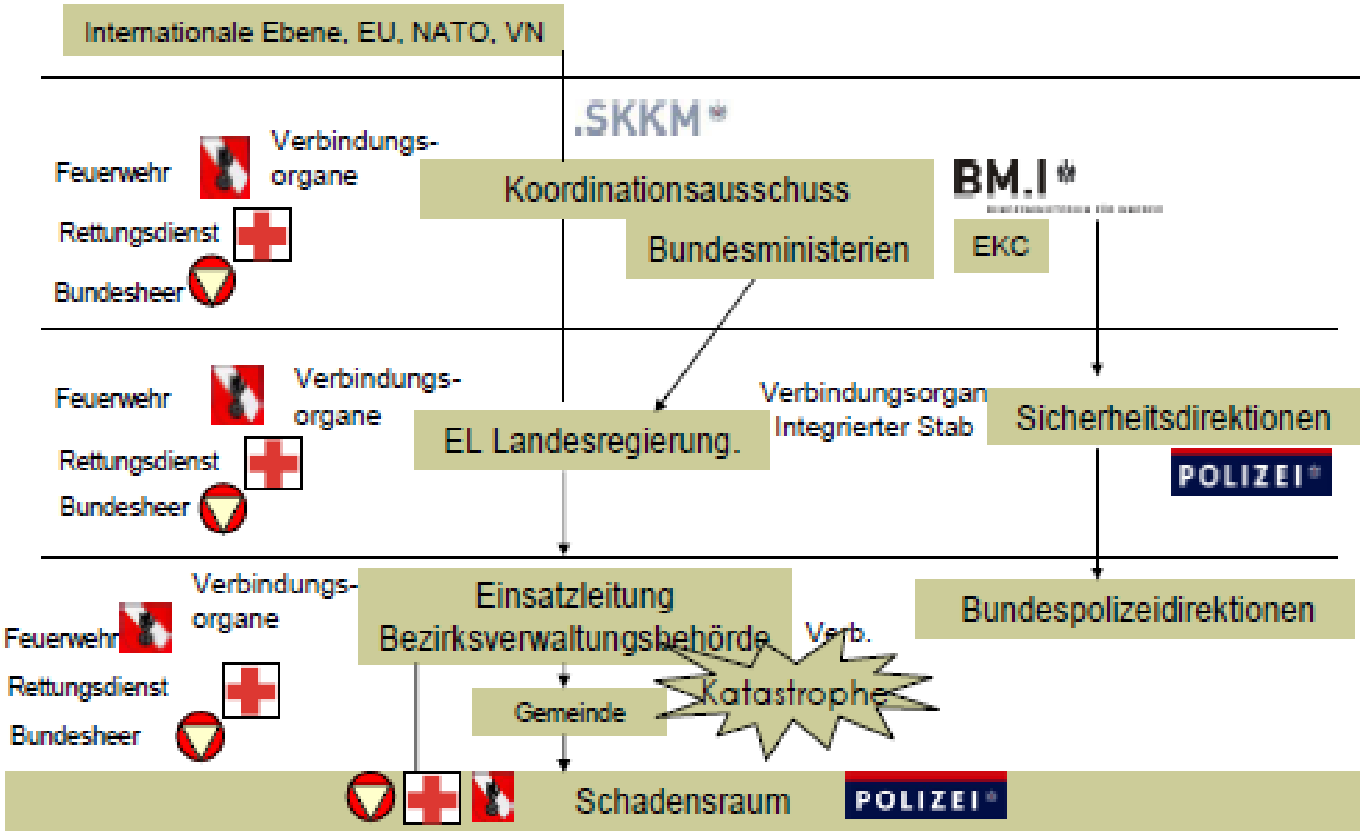
ITSPreventexpert



Quelle BMI

SKKM und Einsatzkräfte

ITSPreventexpert



Quelle BMI

Guidelines für Unternehmen und Betreiber kritischer Infrastruktur

ITSPreventexpert

Netz- und Informationssystemsicherheitsgesetz
NIS2, RKE Resilienz kritischer Einrichtungen

Das NIS 2 und RKE verpflichten Betreiber wesentlicher Dienste und Anbieter digitaler Dienste zur Erhöhung der Sicherheit ihrer Netz- und Informationssysteme.

Krisenkommunikation für Unternehmen intern und zwischen systemrelevanten Betrieben notwendig

Bestehende Informationsquellen und Broschüren

ITSPreventexpert

Bundesministerium Inneres

- Digitaler Aktionsplan
- BMI Ressourstrategie

DIGITAL AUSTRIA

- BMLV Risikobild 2024

Bundesministerium Landesverteidigung

- Broschüre Black Out
- Check- Liste Black Out

WKO NÖ

- Leitfaden Katastrophen Schutzplan
- Maßnahmenkatalog Blackout

Füreinander NIEDERÖSTERREICH

Studienprojekte im Auftrag der Ministerien

ITSPreventexpert

AIT FCC/KIRAS

- **Staatsgrundnetz Bontempiorgel, Hammondorgel,** Vermona Orgel

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY TOMORROW TODAY

ArgoNET

Bundesministerium Landesverteidigung

Bundesministerium Inneres

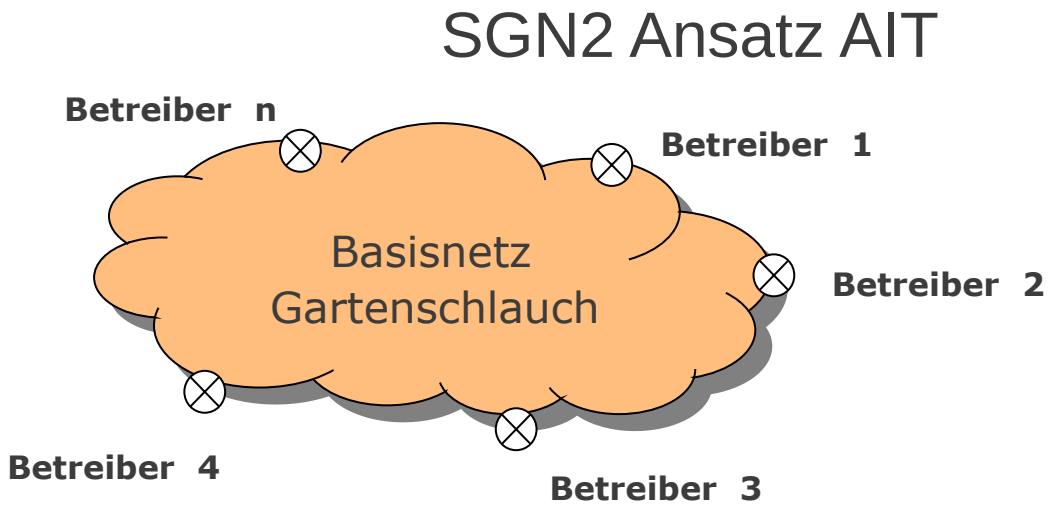
Bundeskanzleramt

Bühler

NOKIA

ITSPreventexpert

universität wien



- **IMPULS -** KLIMAWANDEL UND AUSWIRKUNGEN AUF DEN INFRASTRUKTURBEREICH und KOMMUNIKATIONSNETZE
- **AQUS** Schutz kritischer Infrastruktur in Österreich Glasfasernetzen

Initiativen Landesebene & Zukunftstechnologien

ITSPreventexpert

- **NÖ** Leitfasen zur Erstellung eines Sonderkatastrophenschutzplans

  Strom- und Infrastrukturausfall WKNÖ und ZSVNÖ

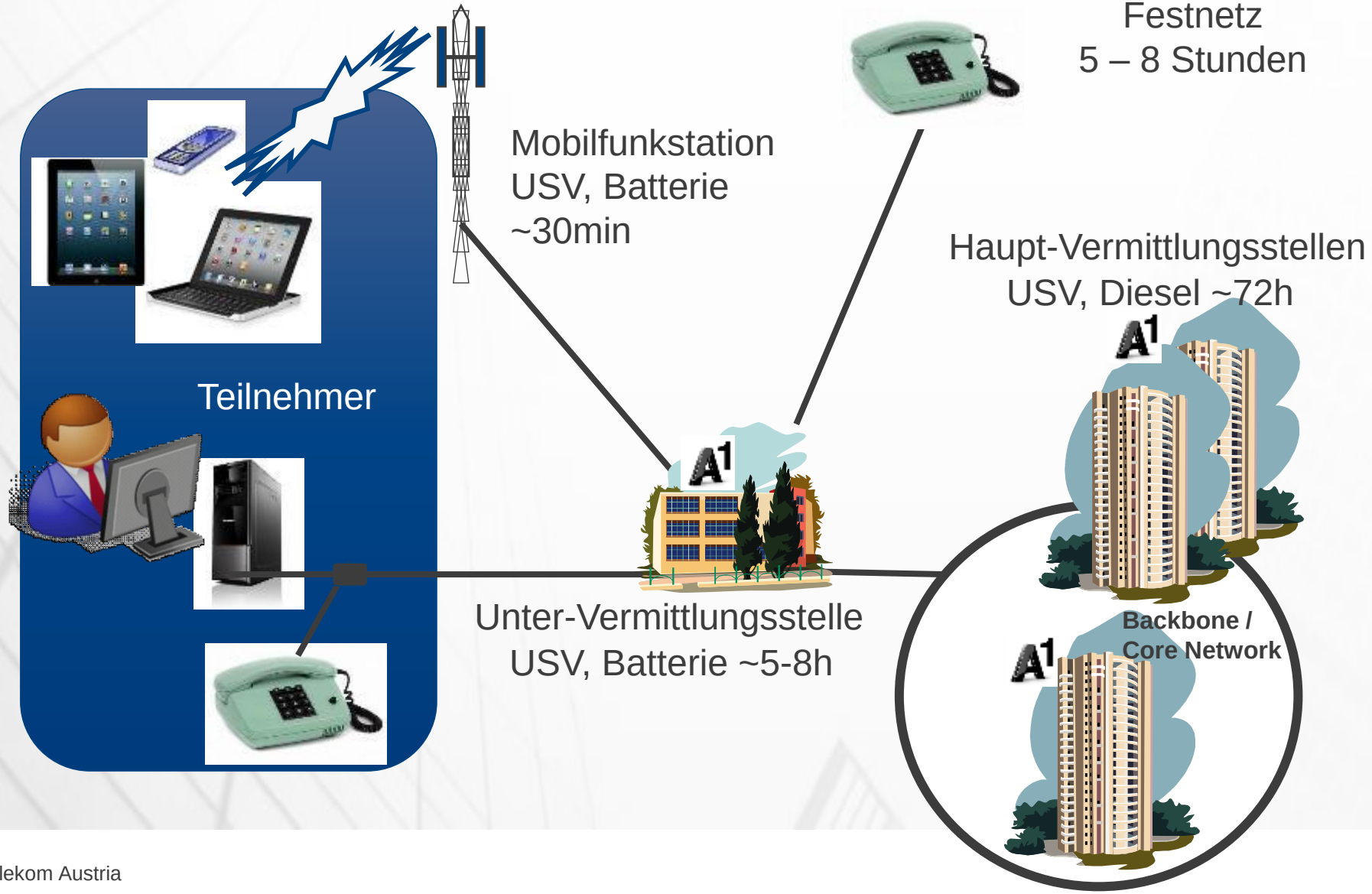
- **QCI- CAT –** Europaweites Projekt Quantenkryptographie in Glasfasernetzen

- **Q-Crit** Austria- Implementiereung eines QKD- Systemes auf einer GF- Weitverkehrsstrecke eines Unternehmens mit kritischer Infrastruktur

Worst Case: Black Out

- Bei längerem Stromversorgungsausfall ist nach nur 30 Minuten keine ausreichende Kommunikation sowohl über Festnetz- und Mobilfunknetz möglich
- Sprachtelefonie, Datenübertragung, Zugang ins Internet und zu Daten die in Cloudservern gehosted sind, sind nicht mehr verfügbar.
- BOS- Funk wird von Blaulichtorganisationen verwendet und steht nicht für die notwendige interne Kommunikation ausreichend zur Verfügung
- Funknetze alleine reichen nicht- mangelnde Störsicherheit, nicht abhörsicher, Witterungsabhängigkeit

Generelle Stromversorgung



Quelle: A1 Telekom Austria

…nach 72 h!

Zur Telekommunikation verbleiben:

- Direkt-Leitungen auf Kupferkabel im Ortsgebiet mit OB-Apparaten und geladener Batterie
- Regionale Funkgeräte mit Batterie/NOA-Versorgung
- Amateurfunkgeräte mit Batterie/NOA-Versorgung
- Botendienste

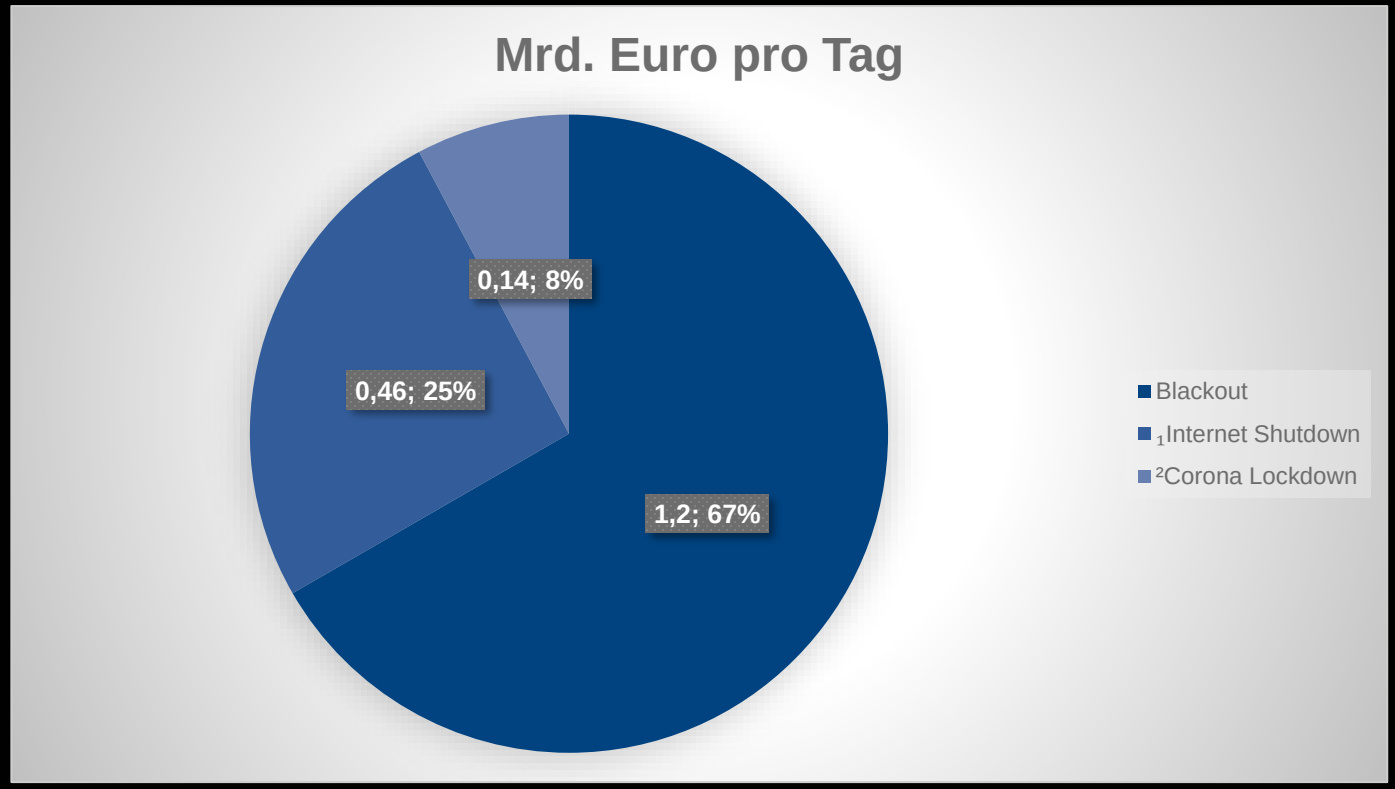
Auswirkung der Digitalen Transformation/

Erfahrungsbericht WKNÖ und ZSVNÖ

- Kein Internet, keine Sprach/Daten/Video Kommunikation
- Auswirkungen eines Black Out auf die Kommunikationsmöglichkeiten bei Bevölkerung aber auch bei Behörden/Kommunen und Führungspersonal in Krankenanstalten, Pflegeheimen und Unternehmen nicht bekannt.
- Die Nichtverfügbarkeit von Mobil- und Festnetz vor allem für die Erreichbarkeit in Notfällen, der fehlende Internetzugang und der Zugang zu den in der Cloud abgespeicherten Daten wird als dramatisch angesehen.
- BOS- Funk alleine genügt nicht.
- Kommunikation für Krisenorganisationen muss funktionieren.
- Pflegeheime und Spitäler müssen untereinander und mit Behörden kommunizieren können.
- Kommunikation für Unternehmen muss gewährleistet sein
- Guidelines und Pläne für Prävention, während der Krise und bei Wiederherstellung notwendig.
- **Masterplan für Kommunikation gefordert.**

ITSPreventexpert

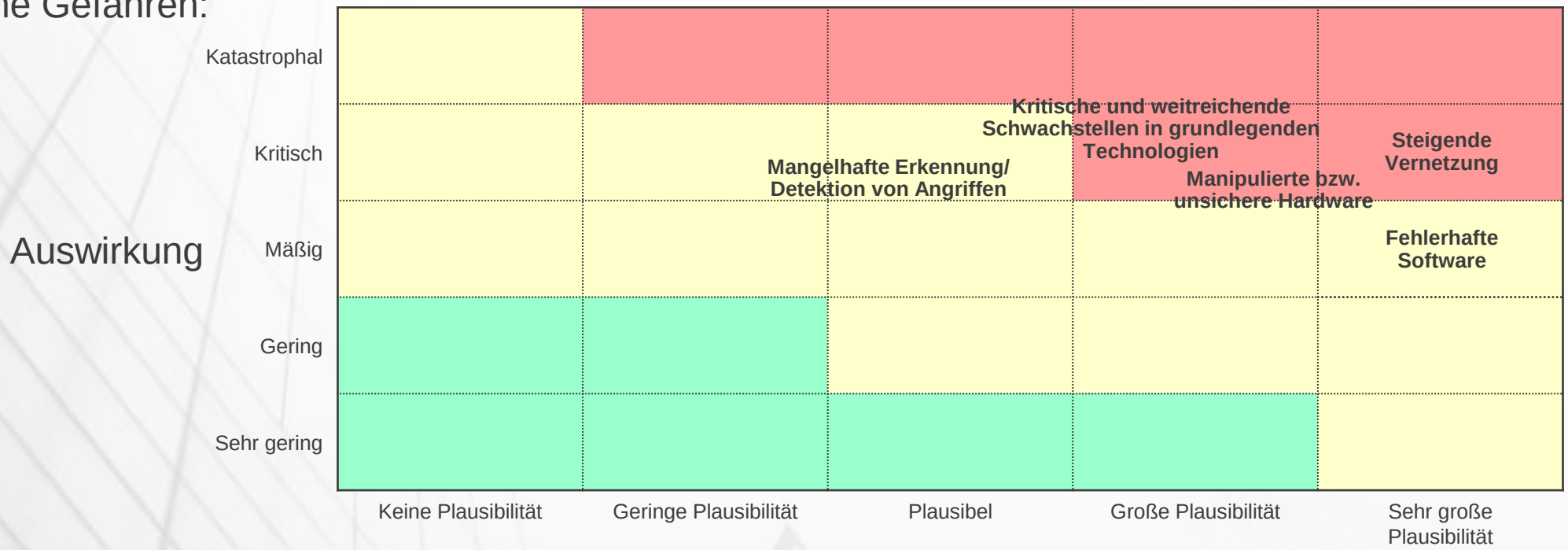
Wirtschaftlicher Schaden in Österreich pro Tag



Risikoanalyse SKI – 2017 / NIS-Gesetz
Gefahrenpotentiale

ITSPreventexpert

- Von der Natur ausgehende Gefahren
- Von Menschen aus kriminellen oder terroristischen Motiven ausgehende Gefahren
- Sonstige von Menschen ausgehende Gefahren
- Technische Gefahren:

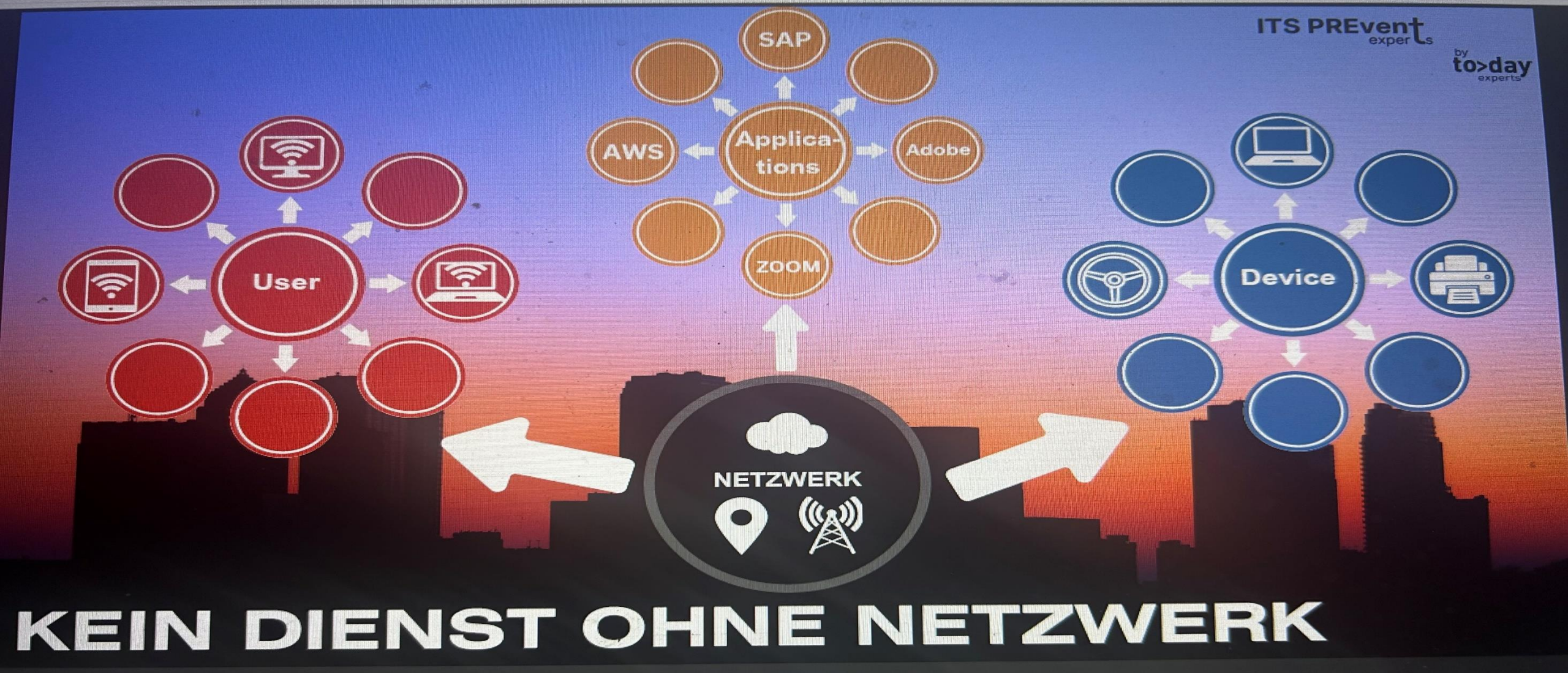


- Quelle BMI

Problematik:

Gefahrenpotentiale durch neue Digitalisierung und neuer Technologien
Internet, Cloud, künstliche Intelligenz

- Bei längem Stromversorgungsausfall ist nach nur 30 Minuten keine ausreichende Kommunikation sowohl über Festnetz- und Mobilfunknetz möglich
- Sprachtelefonie, Datenübertragung, Zugang ins Internet und zu Daten die in Cloudservern gehosted sind, sind nicht mehr verfügbar.
- BOS- Funk wird von Blaulichtorganisationen verwendet und steht nicht für die notwendige interne Kommunikation ausreichend zur Verfügung
- Funknetze alleine reichen nicht- mangelnde Störsicherheit, nicht abhörsicher, Witterungsabhängigkeit

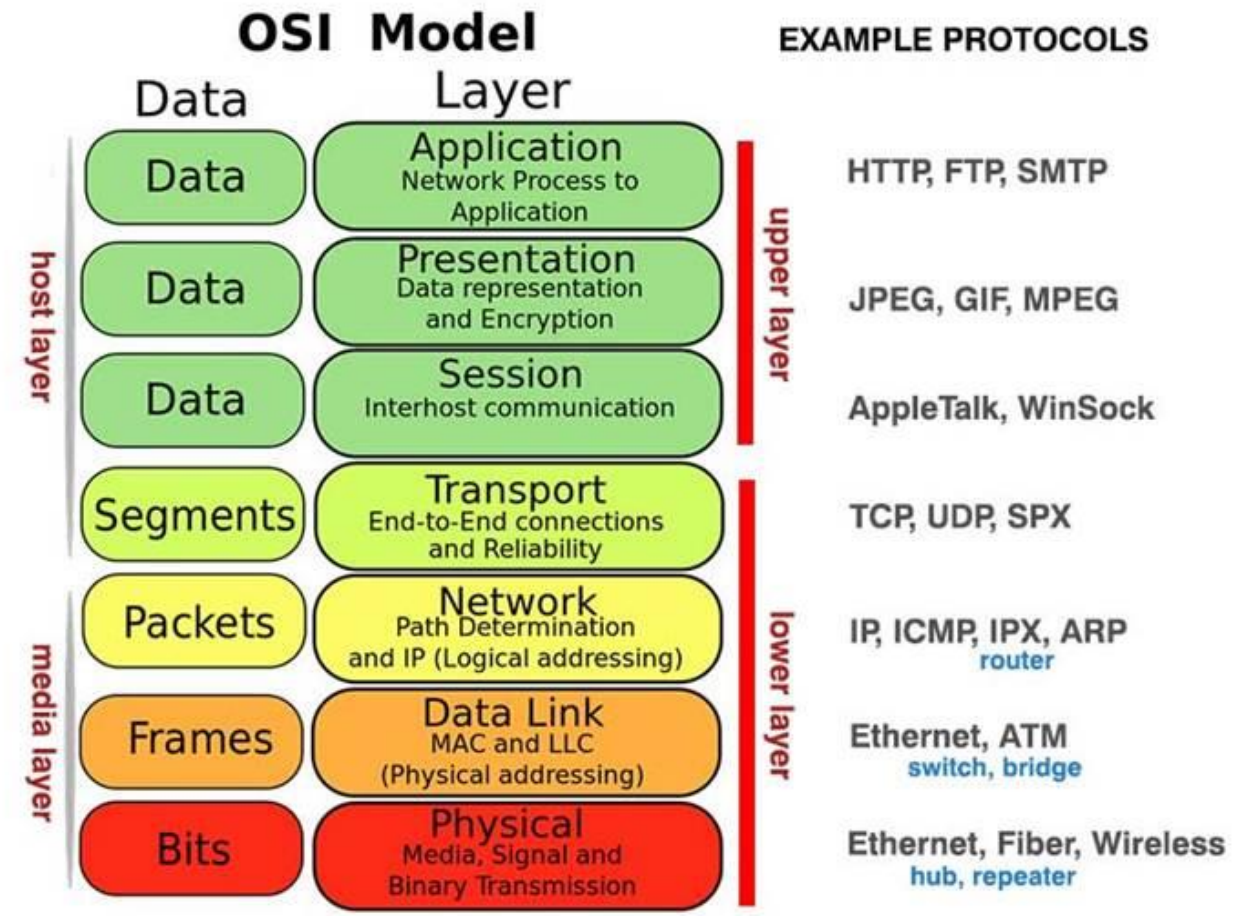


Quelle Fortinet

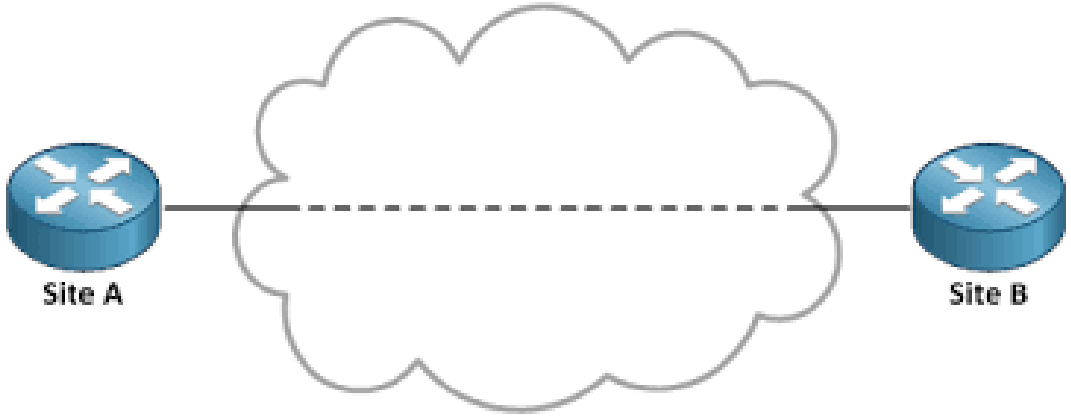
ITSPreventexpert

Kostenfaktor, Gefährdungsanteil Infrastruktur

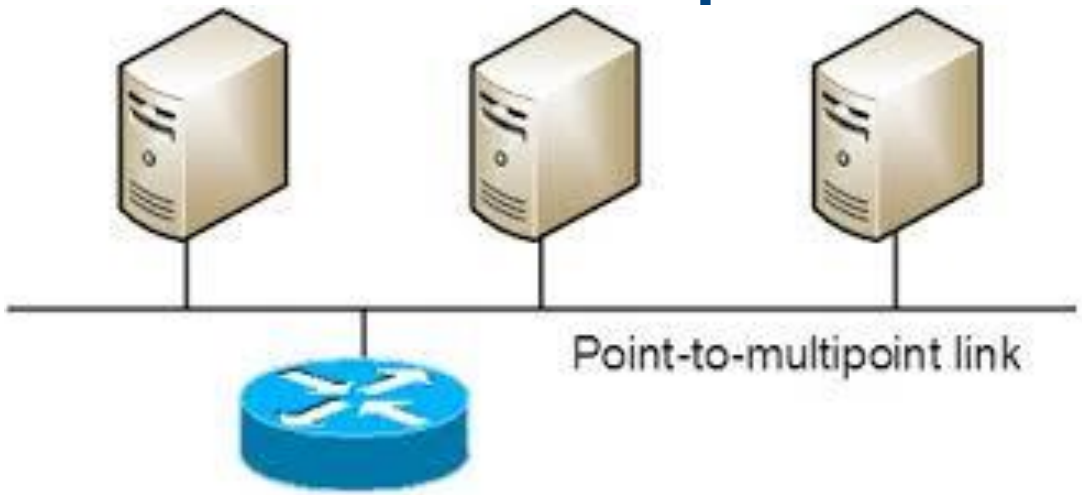
ITSPreventexpert

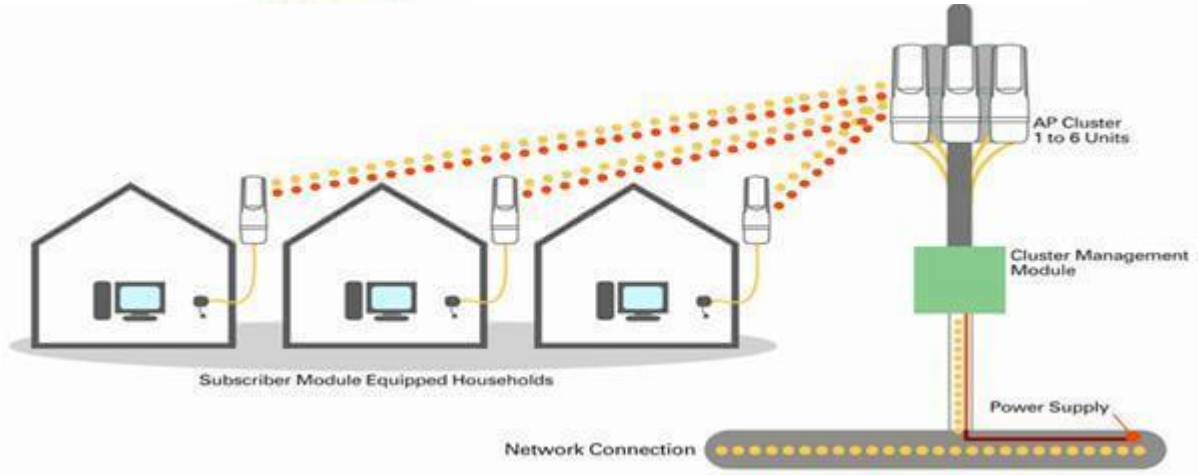


Point to Point



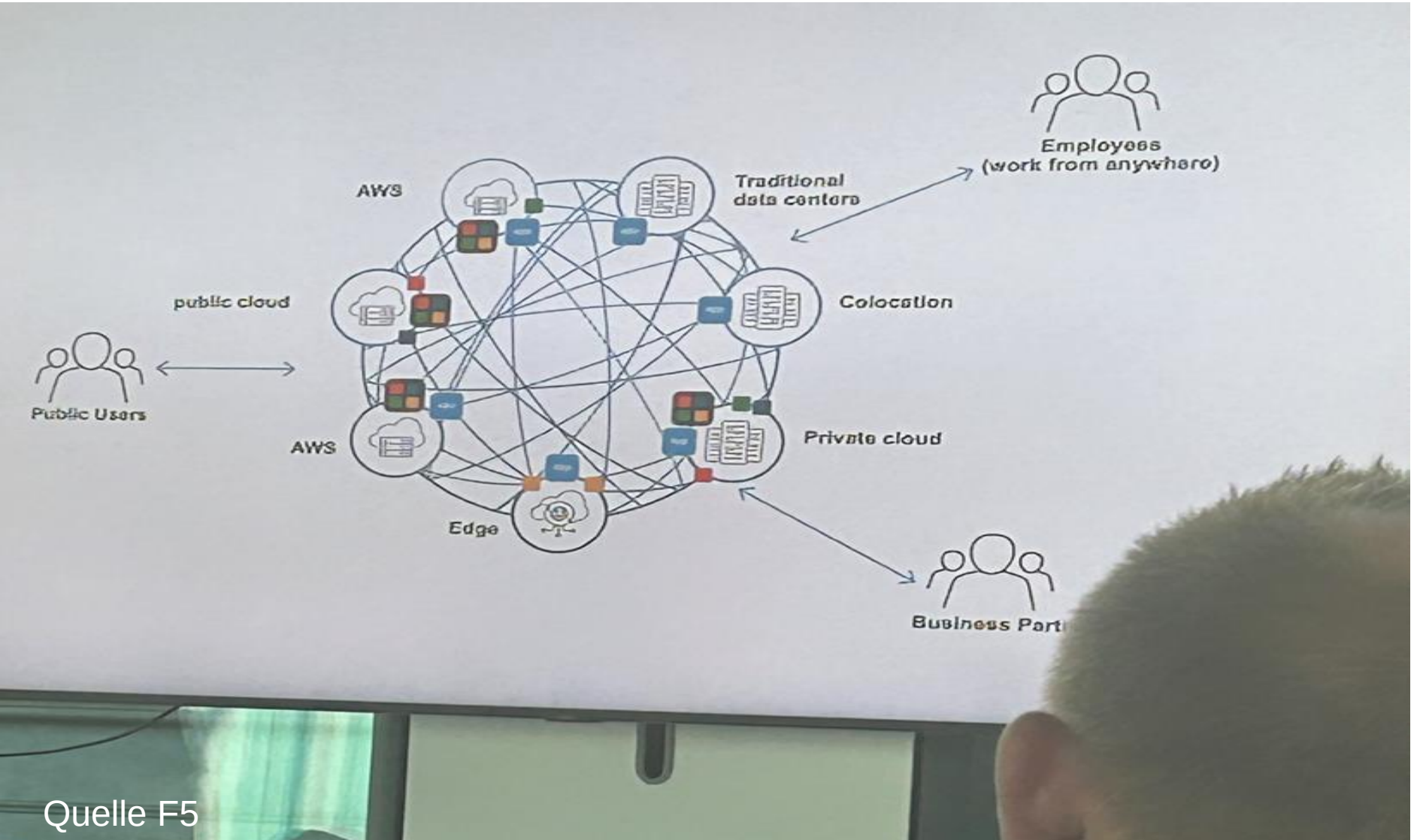
Point to Multipoint





API Application Programming Interface

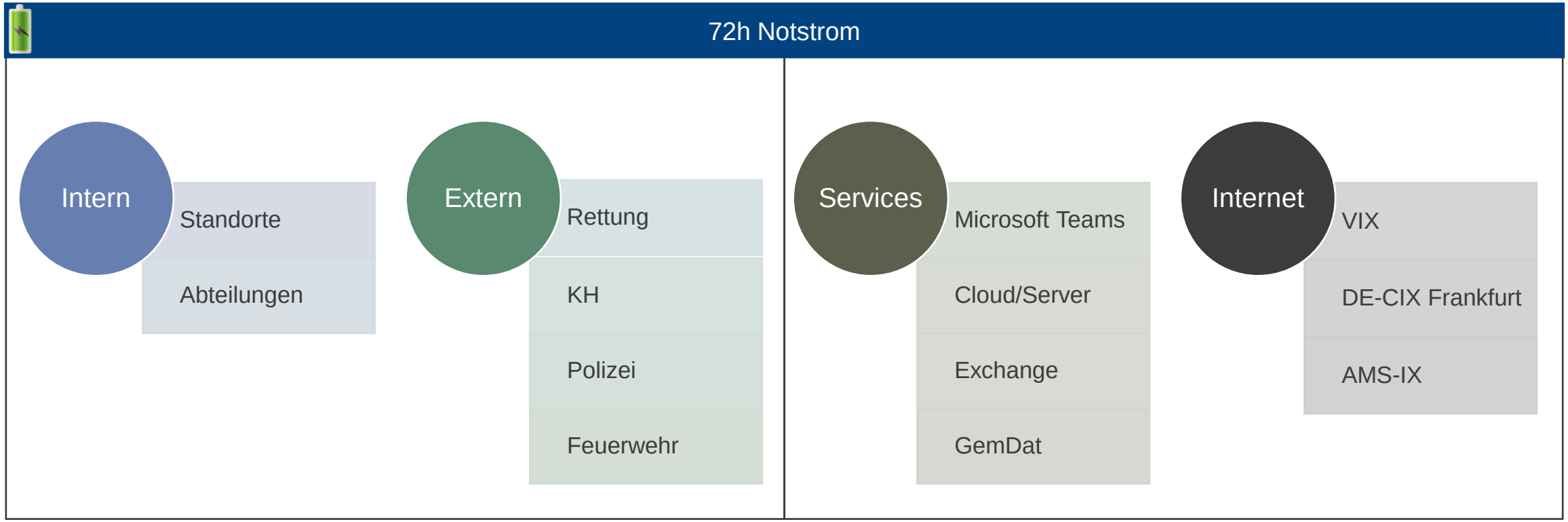
ITSPreventexpert



Quelle F5

4W Evaluierung

Wer kommuniziert mit **Wem**-
Wohin- mit **Welchen** Service?



- Festlegung der Bedarfsträger
- Kommunikationsflüsse/Übertragungswege Intern- und Extern (Kommunikationsmatrix)
- Benötigte Services im Krisenfall (Servicematrix)
- Anzahl und geogr. Zuordnung der notwendigen Übergangspunkte NNI (Topologiematrix)

Abhilfe/Lösungen

Unabhängigkeit von Publik Internet und Cloudzugängen schaffen: Autarke Infrastruktur

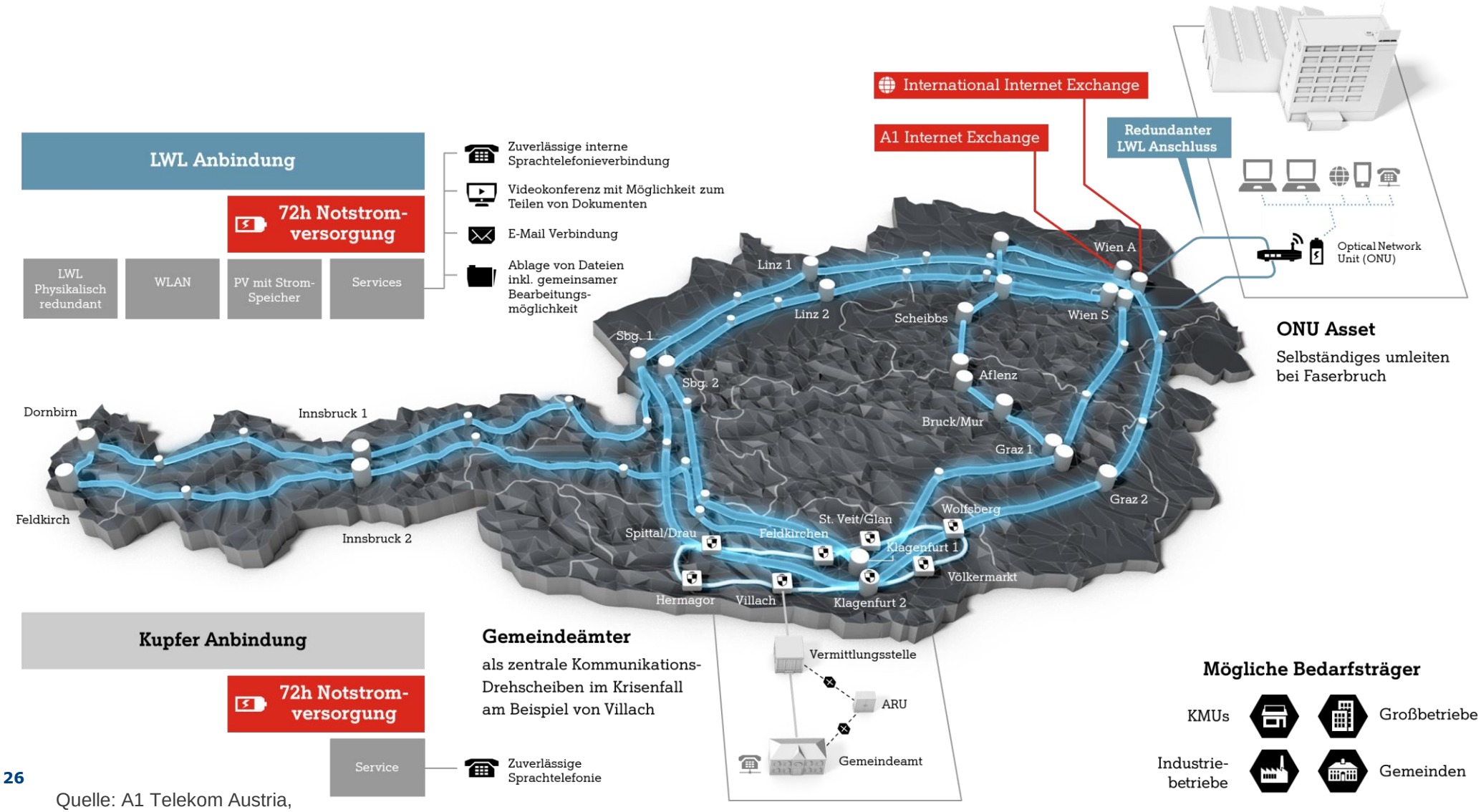
- Bei längem Stromversorgungsausfall ist nach nur 30 Minuten keine ausreichende Kommunikation sowohl über Festnetz- und Mobilfunknetz möglich
- Sprachtelefonie, Datenübertragung, Zugang ins Internet und zu Daten die in Cloudservern gehosted sind, sind nicht mehr verfügbar.
- BOS- Funk wird von Blaulichtorganisationen verwendet und steht nicht für die notwendige interne Kommunikation ausreichend zur Verfügung
- Funknetze alleine reichen nicht- mangelnde Störsicherheit, nicht abhörsicher, Witterungsabhängigkeit

A1 Enterprise Resilience Network

Resilienz für die digitale Infrastruktur Österreichs

ITSPreventexpert

Bestehender A1 Glasfaserring als Basis für höchste Redundanz



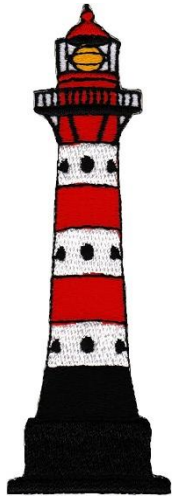
Quelle: A1 Telekom Austria,

Autarke Krisenkommunikation (ohne Internet und Cloudzugang)

Betriebe mit kritischer Infrastruktur, Behörden, Kommunen, Campuslösung für Unternehmen

ITSPreventexpert

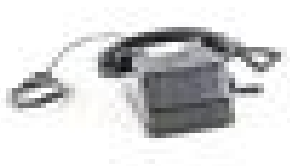
Leuchtürme
Lichtpunkte



- **Behördenfunk BOS:** Vorwiegend für Blaulichtorganisationen
- **WLAN:** nur Daten
- **Satellitenfunk:** benötigt Bodenstation
- **Amateurfunk:** eingeschränkter Personenkreis
- **Handfunkgeräte:** in begrenztem Umkreis

Kabelgebundene Kommunikation

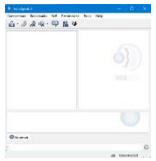
@ **Copper ,** Copper Manufacture



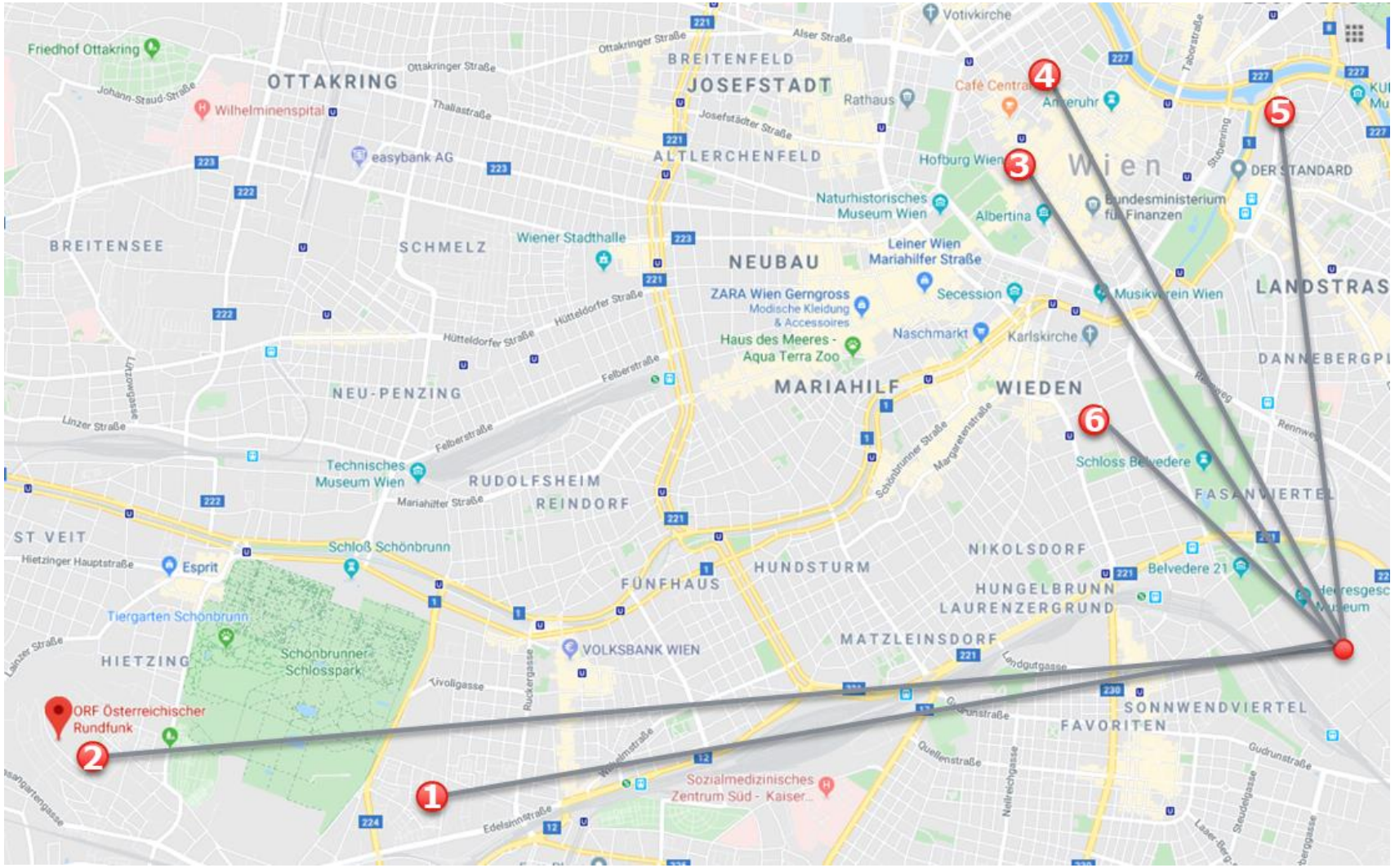
Vorteil: funktioniert auch noch nach 72h hat kleine Ortsbatterie

@ **Fiber**

- Direkte Verbindung über LWL (u.a. im Zuge der LWL Verlegung)
- Über öffentliches Netz wo möglich



Beispiel von Direktleitungen



1. BMI NOC

   Hohenbergstrasse 1

2. ORF

   Würzburggasse 30

3. BMI EKC

   Minoritenplatz 9

4. Berufsfeuerwehr Wien

   Am Hof 9

5. Rettungszentrale Wien *Radetzkystrasse 1*

6. ORF

   Argentinierstrasse 30a

Quelle: A1 Telekom Austria,

Sicherheitspaket Blackout Gemeinden

ITSPreventexpert

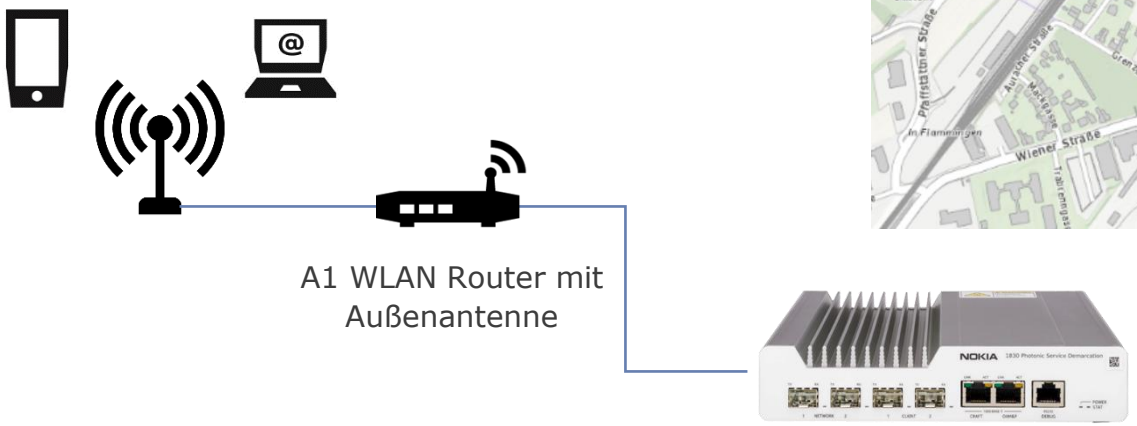
Notkommunikation von Telefonzellen

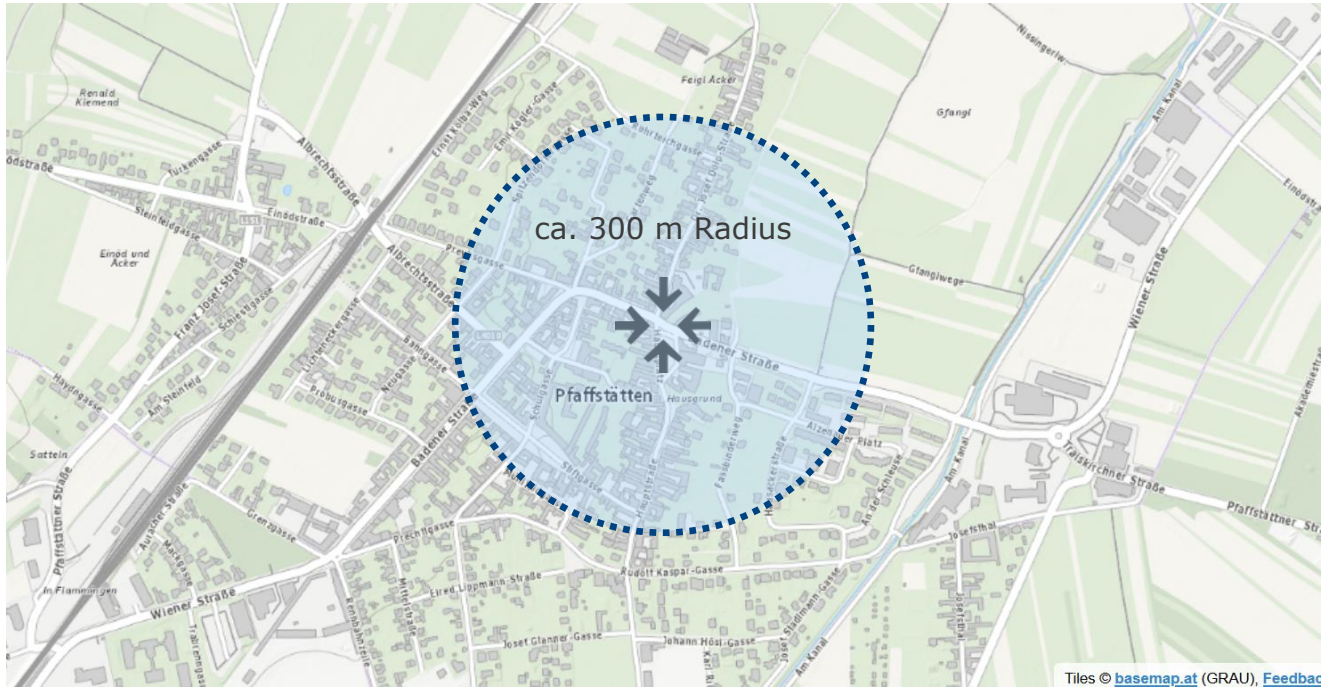
Anbindung wichtiger Bedarfsträger, Hauptstandorte, Infostellen, Selbsthilfebasen
Autarkes Sicherheitsnetz für Krisenstäbe

Mission Future Standort
Gesicherte Stromversorgung bis zu 72h

Quelle: A1 Telekom Austria,

WLAN für die Notfallkommunikation – Anbindung an A1 Glasfaserring notwendig





Input vom NÖ Zivilschutzverband

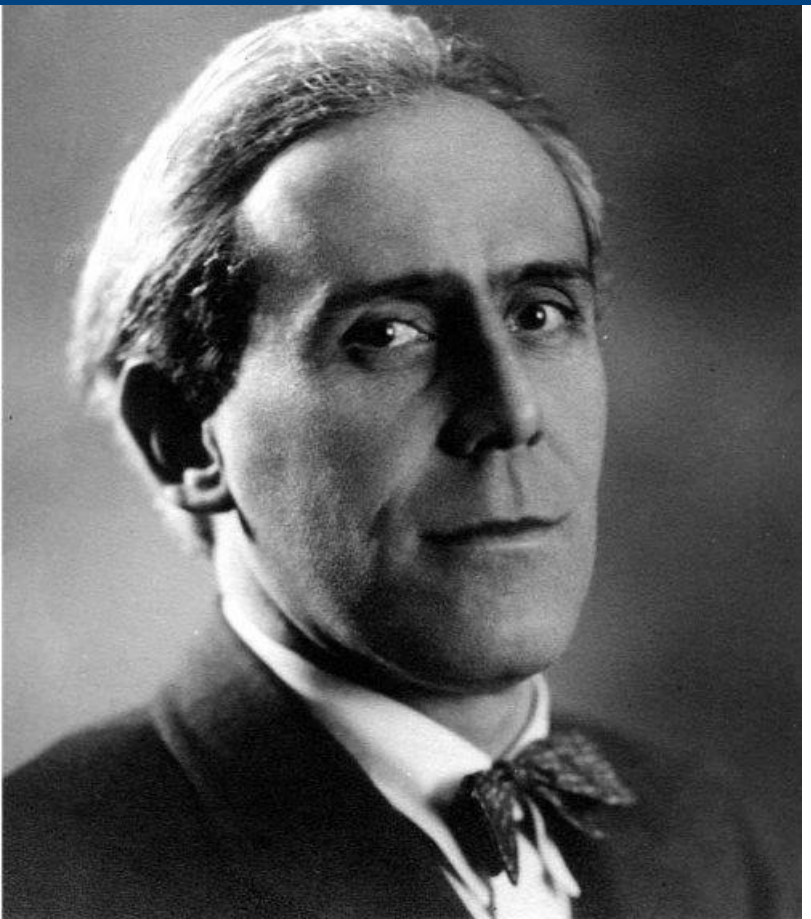
Quelle: A1 Telekom Austria,

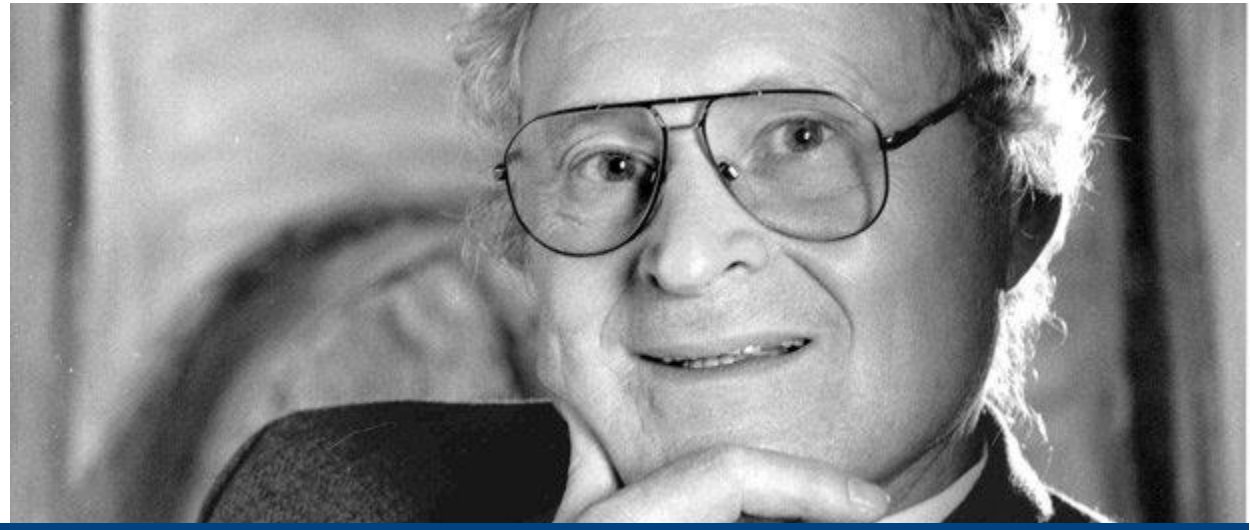
Wozu Krisen- und Notfallmanagement?

ITSPreventexpert

„Es ist unmöglich, dass das Unwahrscheinliche nie geschieht“

Emil Gumbel, Professor für Statistik (1891-1966)





„Man soll rechtzeitig drauf schaun…“

Joki Kirschner (1931-2016)

WOZU investieren???

ITSPreventexpert

Wie oft passiert etwas?
Zu hohe Kosten für Prävention – das Risiko gehen wir ein!

- **Zur Gewährleistung der gesetzlichen Vorgaben**
- **Zum Schutz der Firma**
  - Zum Schutz der Mitarbeiter und Menschenleben
  - Zum Schutz der Basisinfrastruktur und des Business
  - Zum Schutz von Sachgütern und Kapital
  - Zum Schutz der Existenz der verantwortlichen Führungskräfte
  - Zum Schutz der Existenz der Firma

Ist man genügend vorbereitet?

ITSPreventexpert

- Krisenstab
- Erreichbarkeit der notwendigen Personen in Krise
- Kommunikationsinfrastruktur
- Kriterien ab wann Aktionen notwendig sind
- Aufzeichnungen über neuralgische Punkte
- Vorgegebene Abläufe / Prozesse
- Trainings
- Maßnahmen zur raschen Wiederherstellung der Dienstleistungen und Services
- Back Up, Restore, Definition und Ausarbeitung von Wiederanlaufszenarien

Kosten im Vergleich – Risikobewertung

ITSPreventexpert

Präventive Maßnahmen

- Risikomanagement
- Business Continuity Management
- Krisen/Notfall-Management
- Übungen
- Investitionen in Infrastruktur
- …

Desaster

- Fahrlässige Handlung
- Haftung
- Verdienstentgang
- Imageverlust
- Konkurs
- …

Eintrittswahrscheinlichkeit % * Schadenshöhe € = Risikowert €

ITSPreventexpert

Summery/To Do:

- Evaluierung der bestehender Infrastruktur- Netzbetreiber übergreifend
- Installation autarker Kriseninfrastruktur- durch unabhängige, fachkundige Experten
- Durchführung regelmäßiger Krisenübungen zur Kontrolle der funktionierenden Kommunikation und Krisenabläufen

- **Schaffung Kriseninfrastruktur für Behörden, systemrelevante Betriebe, Kommunen, Krankenanstalten, Unternehmen**

ITSPreventexpert

Portfolioerweiterung

- Consulting für autharke Kommunikation
- Evaluierung Connectivity- Netzbetreiber übergreifend
- Revenue Assurance
- Istallation autarker Netzwerke
- BCDR Consulting
- Maßnahmenpläne für Planung, Installation und Betrieb Autharker Netzwerke

Prevention für Ihre Sicherheit

ITSPreventexpert

- Consulting
- Training
- Services
- Risc Prevention
- Cost Reduction

Telefon: +43 664 575 54 34
Email: info@preventexpert.com
www.preventexpert.com

Dipl.HTL.Ing.Leopold Kraus

Unser Portfolio

Consulting für Krisen- und Notfallmanagement

Optimale Gestaltung der notwendigen Abläufe im Krisen- und Notfall
Schwerpunkt Kommunikation und Ausfallsicherheit der Infrastruktur im Krisenfall

ITSPreventexpert

- **Consulting**
- **Training**
- **Business Continuity/ Risc Management**
- **Network Security/IT- Security**
- **Infrastructure/Topologie Management**
- **Krisen/ Notfallmanagement**
- **Disaster Recovery**

Alles aus einer Hand

- Optimale Lösung für sichere Infrastruktur
- Erfüllung der NIS 1 & NIS 2 Kriterien
- Erfüllung der RKE Verordnungen
- Wettbewerbsvorteil bei Ausschreibungen durch Erfüllung Sicherheits- und Krisen/Notfallmanagement Kriterien

Kunden & Geschäftspartner

ITSPreventexpert

ITSPreventexpert

Dipl.HTL.Ing.Leopold Kraus
info@preventexpert.com
www.preventexpert.com