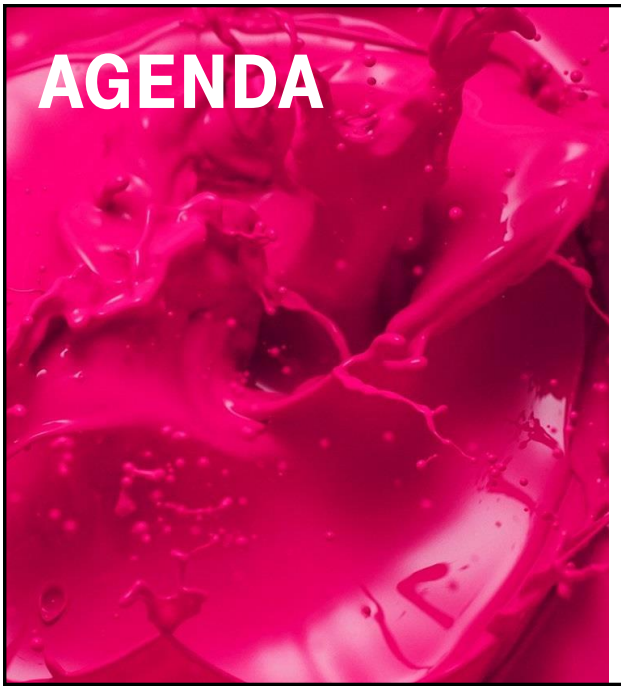
MAGENTA SECURITY INSIDE

KRITISCHE INFRASTRUKTUR SCHÜTZEN JA, ABER WIE?

T-Systems International GmbH | Telekom Security | Emergency & Crisis Management
Symposium Leitstelle aktuell
Bremerhaven, 12. Juni 2018

ERLEBEN, WAS VERBINDET.



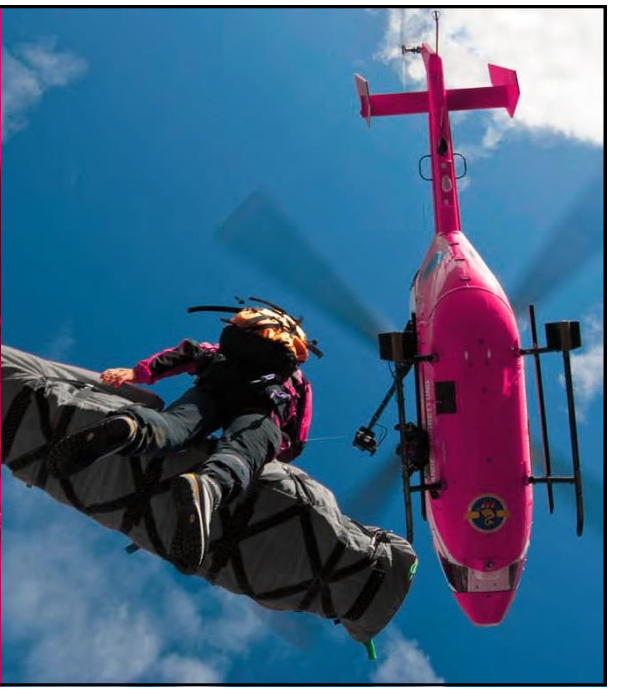
AGENDA

01 Kritische Infrastrukturen

02 Schutz kritischer Infrastrukturen

03 Beispiele aus der Praxis

KRITISCHE INFRASTRUKTUREN



KRITISCHE INFRASTRUKTUR – SCHÜTZEN JA, ABER WIE?
DEFINITION KRITIS

Sektor Staat und Verwaltung

- Regierung und Verwaltung
- Parlament
- Justizeinrichtungen
- Notfall-/Rettungswesen einschließlich Katastrophenschutz

Quelle: www.kritis.bund.de

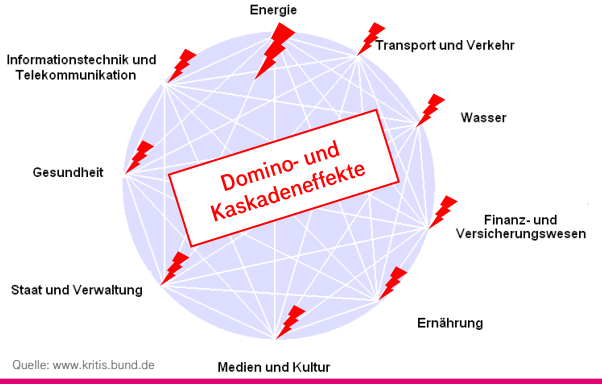
BSI-Gesetz § 2 Abs. 10

Kritische Infrastrukturen **im Sinne dieses Gesetzes** sind Einrichtungen, Anlagen oder Teile davon, die
1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören [...]

Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. (BMI 2009)

KRITISCHE INFRASTRUKTUR – SCHÜTZEN JA, ABER WIE?

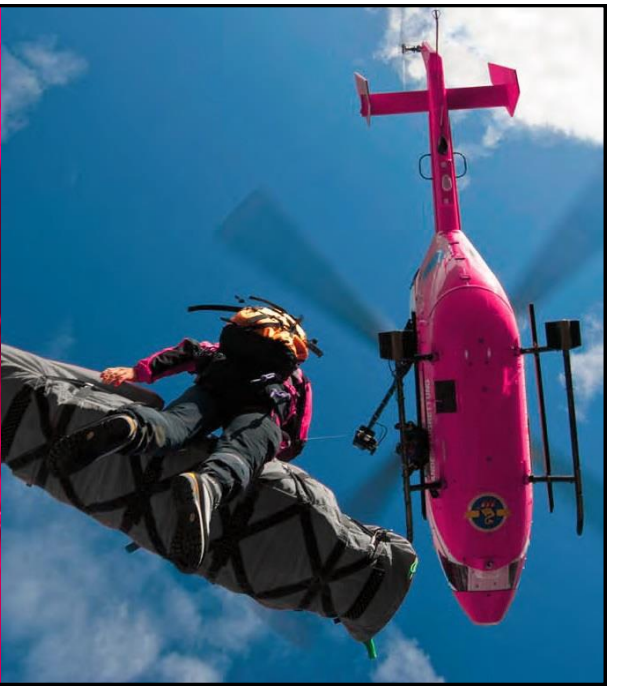
INTERDEPENDENZEN ZWISCHEN DEN SEKTOREN



Quelle: www.kritis.bund.de

Beim Schutz kritischer Infrastrukturen sind insbesondere die gegenseitigen Abhängigkeiten zwischen den Sektoren zu beachten!

SCHUTZ KRITISCHER INFRASTRUKTUREN



KRITISCHE INFRASTRUKTUR – SCHÜTZEN JA, ABER WIE?
WOVOR SCHÜTZEN WIR UNS?

Brand	Geiselnahme
Hochwasser	Krieg
Erdbeben	Gefahrstoffunfall
Epidemien/Pandemien	Stromausfall
Terroranschläge	Cyberangriffe
Erpressung	und viele weitere sowie Kombinationen...

Telekom Router gehackt

Sicherheits-lücken im Speedport

Angriff auf die Telekom

Stecker-zieh-Tag für 900.000 Router

Beispiel: Routerangriff Telekom 2016

Großstörung bei der Telekom: Was wirklich geschah

30.11.2016 14:12 Uhr – Jürgen Schmidt

Der geöffnete Speedport W921V (Bild: Comsecuris, Ralf-Philipp Weinmann)

Ein Sicherheitsexperte hat die Reaktion eines der anfälligen Speedport-Modelle analysiert und kommt zu einer überraschenden Erkenntnis: Die Geräte waren gar nicht anfällig für die TR-069-Sicherheitslücke.

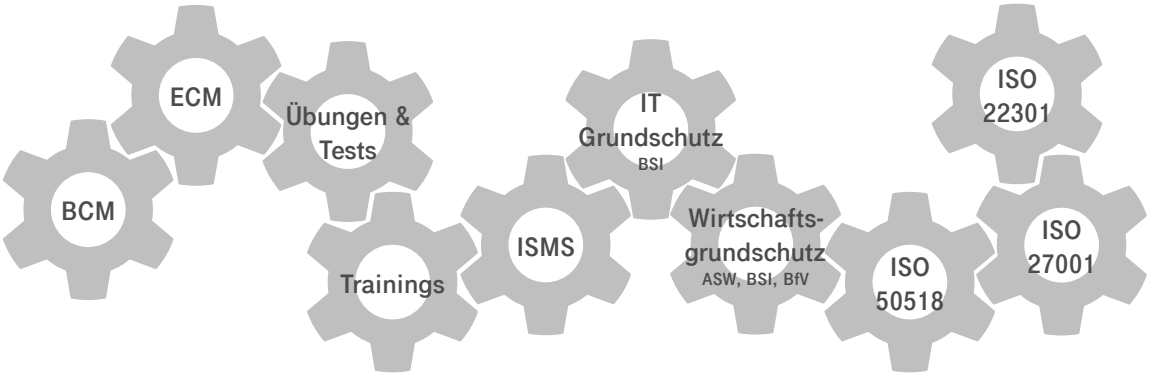
Quelle: https://www.heise.de/security/meldung/Grossstoerung-bei-der-Telekom-Was-wirklich-geschah-3520212.html

KRITISCHE INFRASTRUKTUR – SCHÜTZEN JA, ABER WIE?
DIE WESENTLICHEN SCHRITTE ZUM SCHUTZ VON KRITIS

Planung	▪ Verantwortlichkeiten festlegen, Zustimmung erlangen, Pflichten bestimmen ▪ strategische Schutzziele definieren
Kritikalitäts-/ Risikoanalyse inkl. Bewertung	▪ Kritikalitätsanalyse durchführen ▪ Risiko inkl. Gefahren/Verwundbarkeiten analysieren und bewerten ▪ operative Schutzziele definieren
Vorbereitende und vorbeugende Maßnahmen	▪ Pläne erstellen, z. B. Business Continuity Pläne oder Notfallpläne ▪ Mitarbeiter schulen, Pläne testen, Übungen durchführen
Notfall- und Krisenreaktion	▪ Notfall- und Krisenmanagement implementieren, testen und trainieren ▪ Notfälle und Krisen koordinieren/managen

KRITISCHE INFRASTRUKTUR – SCHÜTZEN JA, ABER WIE?

ES GIBT VIELFÄLTIGE MASSNAHMEN ZUM SCHUTZ DER KRITIS



Methoden und Tools sind gemäß der tatsächlichen Anforderungen auszuwählen und gegebenenfalls zu adaptieren.

BEISPIELE AUS DER PRAXIS

KRITISCHE INFRASTRUKTUR – SCHÜTZEN JA, ABER WIE?
BUSINESS CONTINUITY MANAGEMENT BEI DER TELEKOM

Nichtverfügbarkeit von Gebäuden

Nichtverfügbarkeit von Personal

Nichtverfügbarkeit von Technologie

Nichtverfügbarkeit von Lieferanten

Szenarienbasierte und prozessbezogene Business Continuity Pläne stellen den Betrieb sicher!
Die Pläne enthalten die Maßnahmen für einen Notbetrieb und den Wiederanlauf.

KRITISCHE INFRASTRUKTUR – SCHÜTZEN JA, ABER WIE?
BCM PERSONALAUSFALL BEI DER TELEKOM

Erkrankung

Erkrankungen (z. B. pandemische Grippe oder Noro-Virus) führen zu Personalausfällen in größerem Umfang.

Ausfall Nahverkehr

Ausfall des öffentlichen Nahverkehrs in größerem Umfang führt dazu, dass Mitarbeiter nicht mehr oder stark verspätet zum Arbeitsplatz erscheinen.

Naturereignis

Naturkatastrophen/Extremwetterereignisse führen dazu, dass Mitarbeiter nicht mehr oder stark verspätet zum Arbeitsplatz erscheinen.

Tarifverhandlungen

Streik im Rahmen von Tarifverhandlungen führen dazu, dass Mitarbeiter nicht am Arbeitsplatz erscheinen.

Business Continuity Management Szenario
Nichtverfügbarkeit von Personal

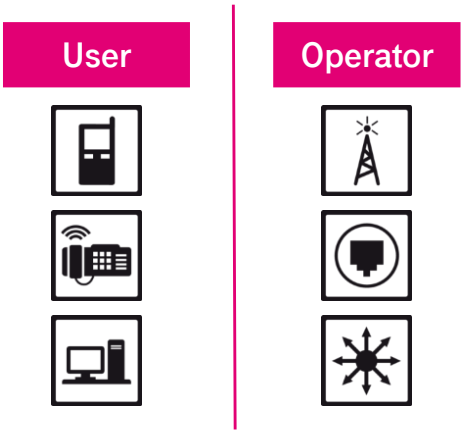
KRITISCHE INFRASTRUKTUR – SCHÜTZEN JA, ABER WIE?
BCM TECHNOLOGIEAUSFALL BEI DER TELEKOM

Disaster Recovery für Festnetz und Mobilfunk

- **Telekommunikationstechnik** in Container-/ Kofferlösungen sowie Kran- und Antennenaufbauten inkl. Netzersatzanlagen
- **24/7 Erreichbarkeit** der Disaster Recovery Management Spezialisten
- **Übungen** und **Realeinsätze**, z. B. bei Events
- **ISMS** nach ISO 27001
- **BCMS** nach ISO 22301 zertifiziert

KRITISCHE INFRASTRUKTUR – SCHÜTZEN JA, ABER WIE?
BCM LIEFERANTENAUSFALL BEI DER TELEKOM

- **Ersatzenergieversorgung** in den zentralen Netzelementen der Telekom gewährleistet die Funktionsfähigkeit auch bei Stromausfall.
  - ortsfeste Netzersatzanlagen
  - mobile/fahrbare Netzersatzanlagen
- Die verfügbare Energiereserve richtet sich nach Bedeutung und Größe des Netzelements.
- Ausreichende **Energieversorgung** als Beitrag zum Funktionieren des Gemeinwesens ist Aufgabe der **Energieversorger** (KRITIS-Sektor Energie).
- Fragen der **Betankung / Priorisierung des Treibstoff** bei langanhaltendem Stromausfall sind zu klären.



KRITISCHE INFRASTRUKTUR – SCHÜTZEN JA, ABER WIE?
EMERGENCY & CRISIS MANAGEMENT BEI DER TELEKOM

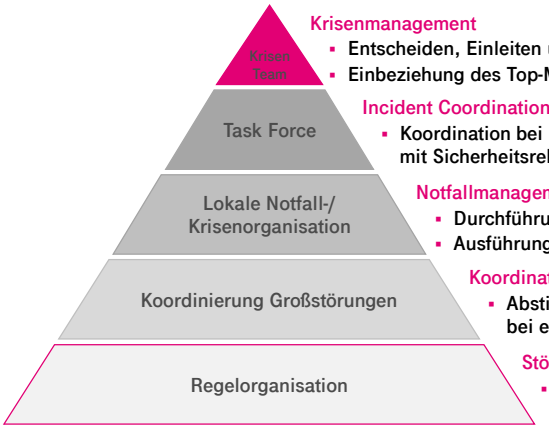
Notfall

- Akute Gefahr oder Ausnahmesituation
- Störung der Betriebsabläufe
- Planmäßige Beseitigung ist aufgrund nicht ausreichender Ressourcen fraglich
- Potentielle Entstehung hoher materieller oder immaterieller Schäden

Krise

- Fortbestand des Unternehmens – ganz oder in Teilen – gefährdet
- Nachhaltige Schädigung des Unternehmens Image des Unternehmens droht
- Geschäftserbringung in starkem Maß beeinträchtigt oder nicht mehr möglich
- Drohende Lebensgefahr oder starke Gefährdung der Gesundheit

KRITISCHE INFRASTRUKTUR – SCHÜTZEN JA, ABER WIE?
EMERGENCY & CRISIS MANAGEMENT BEI DER TELEKOM



Krisenmanagement
- Entscheiden, Einleiten und Kontrolle von Maßnahmen im Krisenfall
- Einbeziehung des Top-Managements

Incident Coordination
- Koordination bei bereichsübergreifenden Incidents und Vorfällen mit Sicherheitsrelevanz bzw. bei Eskalation Notfallmanagement

Notfallmanagement
- Durchführung der Notfallpläne
- Ausführung und Kontrolle der Maßnahmen aus Notfallplan

Koordination Großstörungen
- Abstimmung Kundenprozesse und Kommunikation bei erhöhtem Koordinationsbedarf

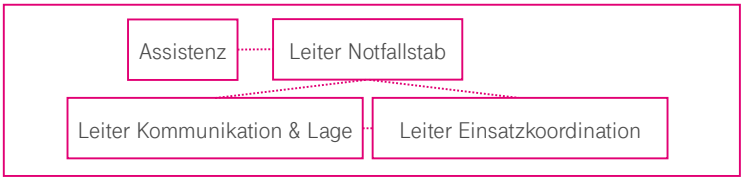
Störungs- und Problembehebung
- Störungsbeseitigung im Regelbetrieb

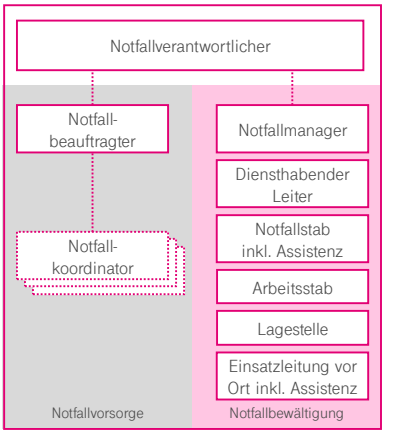
KRITISCHE INFRASTRUKTUR – SCHÜTZEN JA, ABER WIE?
EMERGENCY & CRISIS MANAGEMENT BEI DER TELEKOM

In jeder Organisationseinheit der Deutschen Telekom AG ist eine **Notfallorganisation** etabliert, diese ist für die **Notfallvorsorge** und **Notfallbewältigung** verantwortlich.

Die Notfallorganisation steuert alle Maßnahmen/Regelungen für die Aufrechterhaltung bzw. Wiederherstellung der Funktionsfähigkeit betroffener Systeme beim Eintritt einer Gefahr oder Ausnahmesituation.

Grundsätzlich bewältigt der **Notfallstab** eine Notfallsituation.





KRITISCHE INFRASTRUKTUR – SCHÜTZEN JA, ABER WIE?
LEITSTELLENSERVICE DER DEUTSCHEN TELEKOM

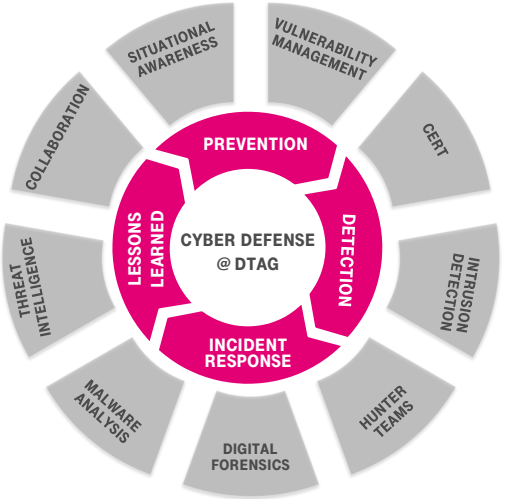
- **First-/Second-Level bei Störungen** an Notrufanschlüssen 110/112:
  Störungsmanagement inkl. Überwachung der Servicelevel
- **Proaktives Störungsmanagement** (Überwachung Schicht 1/2 der Notrufanschlüsse)
  Ein Ausfall der ISDN- bzw. PMX-Anschlüsse wird im Leitstellenservice signalisiert, die Störungsbearbeitung wird proaktiv begonnen.
- **Notrufrückverfolgungen** auch netzübergreifend (bei Nichtermittlung des Anrufers)
- Bundesweiter Zugriff auf Vermittlungstechnik inkl. der Möglichkeit **Anrufweiterleitungen** für Notrufanschlüsse einzurichten
- **Zertifizierung nach VdS 3138**
  (Zutrittskontrolle, beschusssichere Fensterscheiben, Notstrom, Personaleinsatz, Back-Up-Leitstelle etc.)

Sämtliche Notrufanschlüsse bundesweit sind Telekomanschlüsse!

KRITISCHE INFRASTRUKTUR – SCHÜTZEN JA, ABER WIE?
SECURITY OPERATION CENTER DER DEUTSCHEN TELEKOM

Integriertes & flexibles Security Operation Center

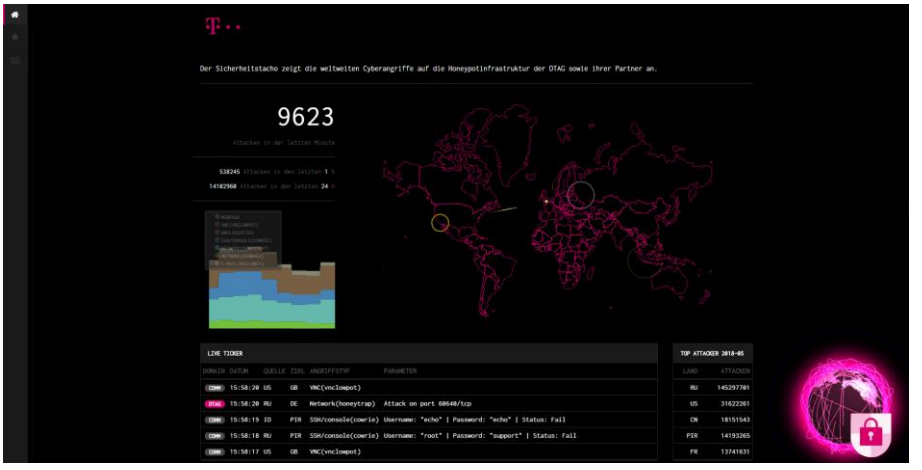
- 24 / 7 / 365
- 16 / 5 / 365
- auf Wunsch Deutschland-only Ressourcen
- sonst Mix Deutschland / Nearshore

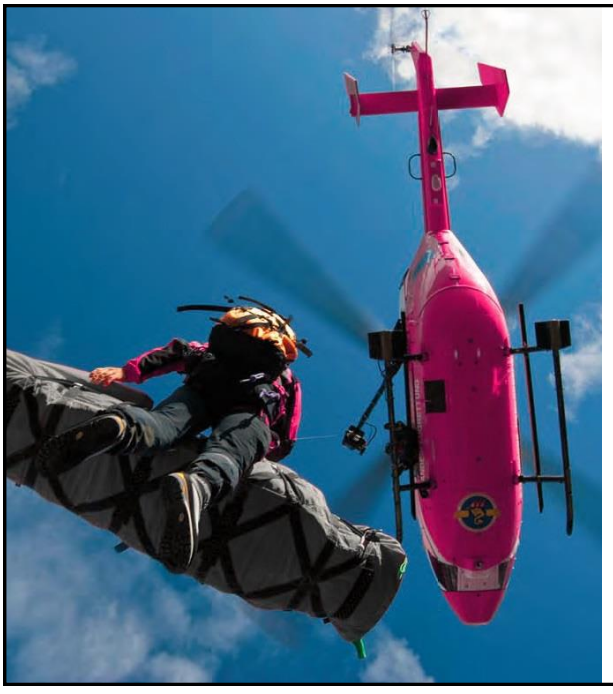


KRITISCHE INFRASTRUKTUR – SCHÜTZEN JA, ABER WIE?
SECURITY OPERATION CENTER DER DEUTSCHEN TELEKOM

KRITISCHE INFRASTRUKTUR – SCHÜTZEN JA, ABER WIE?

WWW.SICHERHEITSTACHO.EU





KONTAKT

Johannes Hartl

Expert Security
Emergency and Crisis Management

T-Systems International GmbH
Telekom Security
Godesberger Allee 83-91
53175 Bonn
Germany

Phone: +49 228 181-57447
Mobile: +49 160 90193525
E-Mail: johannes.hartl@t-systems.com

www.telekom.de/security