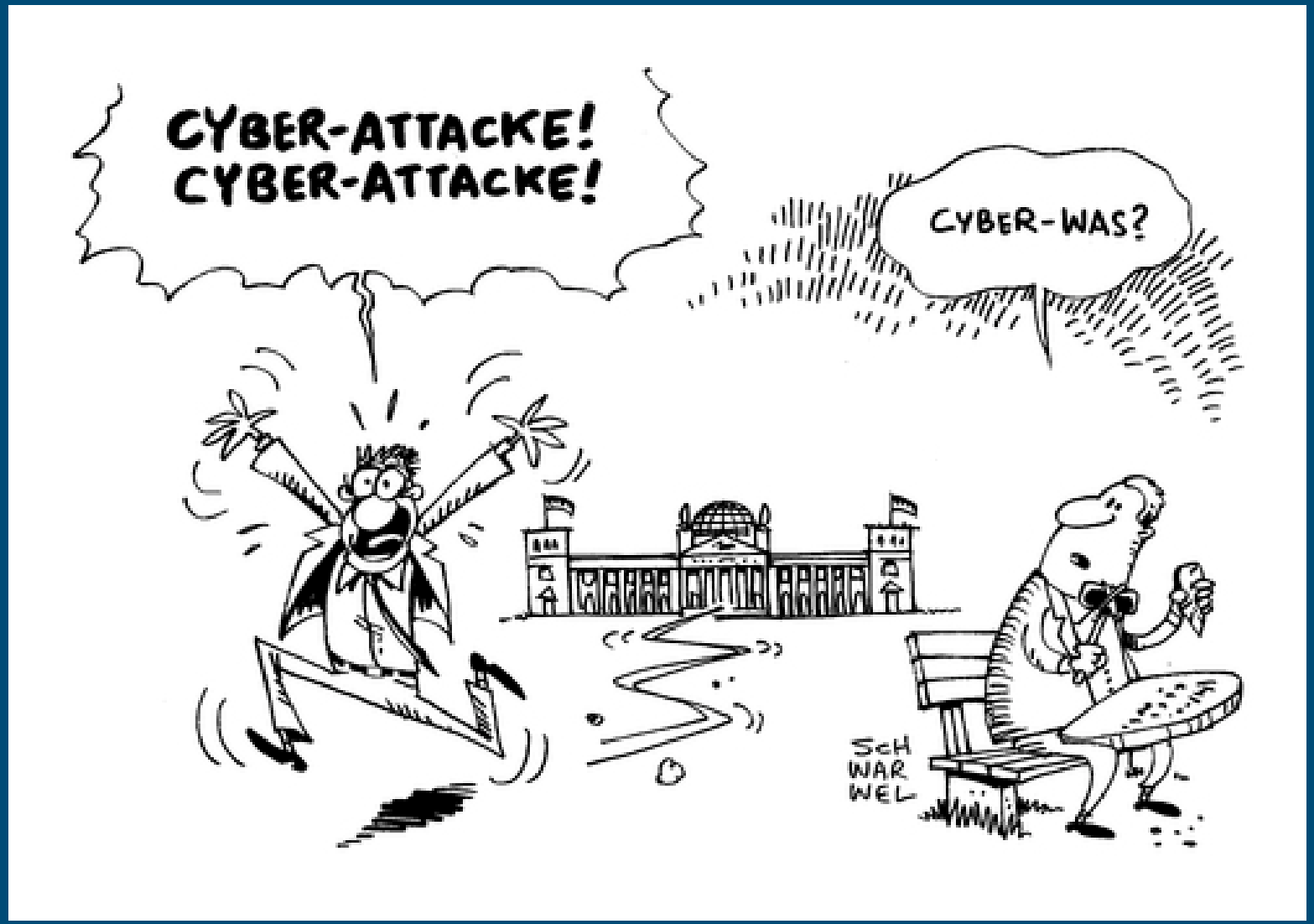
Cyber-Resilience-Framework

Praktische Hilfestellungen für Kommunen
im Falle von IT-Sicherheitsvorfällen

Bundesamt
für Sicherheit in der
Informationstechnik

Fabienne Tegeler (BSI), 04.11.2025

Vis!t 2025, Linz



https://de.toonpool.com/cartoons/Cyber%20Attacke%20Bundestag%20Hacker_249528

Agenda

- Dialog für Cybersicherheit
- Workstream „Cyber-Resilience-Framework. In IT-Krisen schneller agieren. (RESI)“
- Was steckt im Framework?
- Struktur und Anwendung
- Das Szenario – Eine Blaupause für den Ernstfall
- Ergebnisse
- Ausblick

Bundesamt für Sicherheit in der Informationstechnik

Dialog für Cyber-Sicherheit

Dialog für Cybersicherheit

- Digitalisierung
- Vernetzung
- Innovationen

BSI

Multistakeholder-Dialog

- Staat 
- Wissenschaft 
- Wirtschaft 
- Kultur und Medien 
- Zivilgesellschaft 

Cybersicherheit – alle Perspektiven einbeziehen

https://www.dialog-cybersicherheit.de

Workstream „Cyber-Resilience-Framework. In IT-Krisen schneller agieren. (RESI)“

Vision: Stärkung von Kommunen, damit diese im Falle eines Cyberangriffs schneller und effektiv reagieren können

Ziel: Entwicklung eines Resilienz-Frameworks für effizientere Reaktionsprozesse von Kommunen und somit Minimierung der Schäden für Bürger:innen

- Aufbau auf bereits vorhandenen Hilfsmittel, Konzepte und Prozesse
- Schließung von Lücken durch die Entwicklung zielgerichteter Hilfsmittel
- Entwicklung eines fiktiven kommunalen Ransomware-Szenarios als Blaupause

Was steckt im Framework?

Ausgangslage

- IT-Krisen zeigen: **Zusammenarbeit zwischen Verwaltungsebenen ist schwierig**
- Unterschiedliche Prozesse, Methoden, Erwartungen
- Kommunen: hohe Krisenkompetenz aber IT-Krisen oft Neuland
- Föderale Strukturen erschweren schnelle Koordination
- Ziel: **Handlungsfähigkeit & Vertrauen sichern** trotz Chaosphase

Was steckt im Framework?

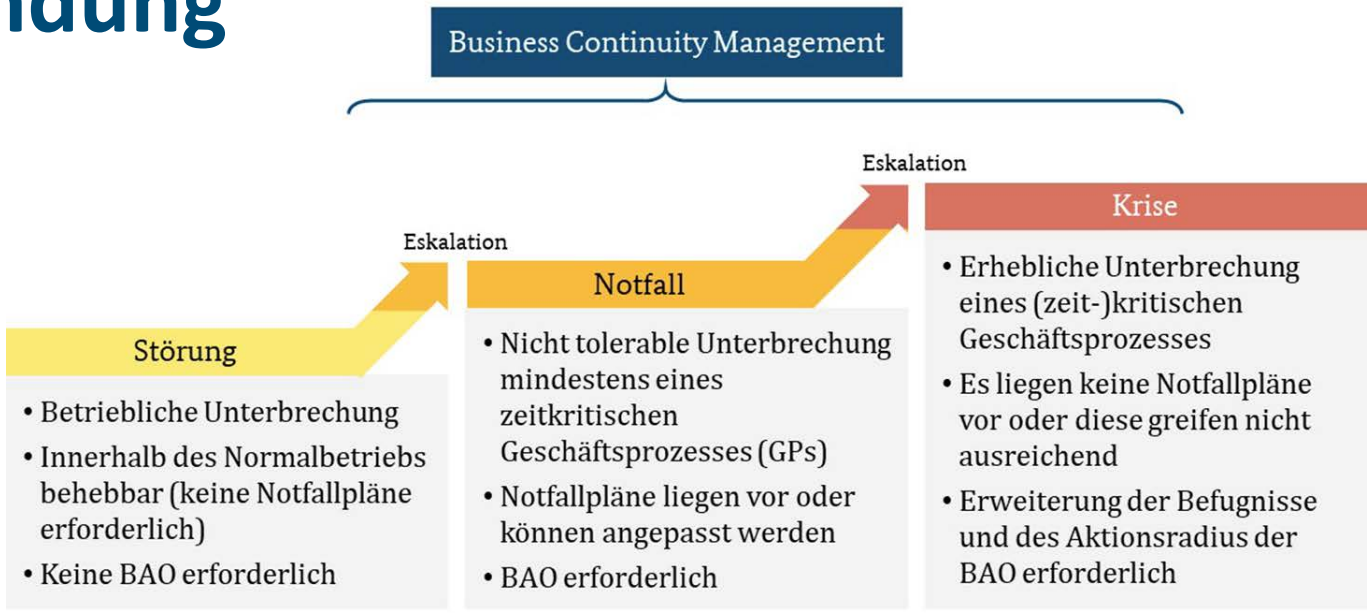
Ziel und Ansatz des Frameworks

- RESI **= strukturelles und konzeptionelles Framework**, das Kommunen bei der **Organisation, Analyse und Bewertung** ihres IT-Krisenmanagements unterstützt
- **Schafft Ordnung & Orientierung** in der Krisenphase
- Bietet: vorgefertigte Komponenten, standardisierte Abläufe, Werkzeuge
- Ziel: **geordnetes Handeln** statt ad-hoc-Reaktionen
- Fokus: **Nutzung & Bündelung bestehender Hilfsmittel**
- Grundlage: BSI-Standard 200-4 (Business Continuity Management)

Struktur und Anwendung

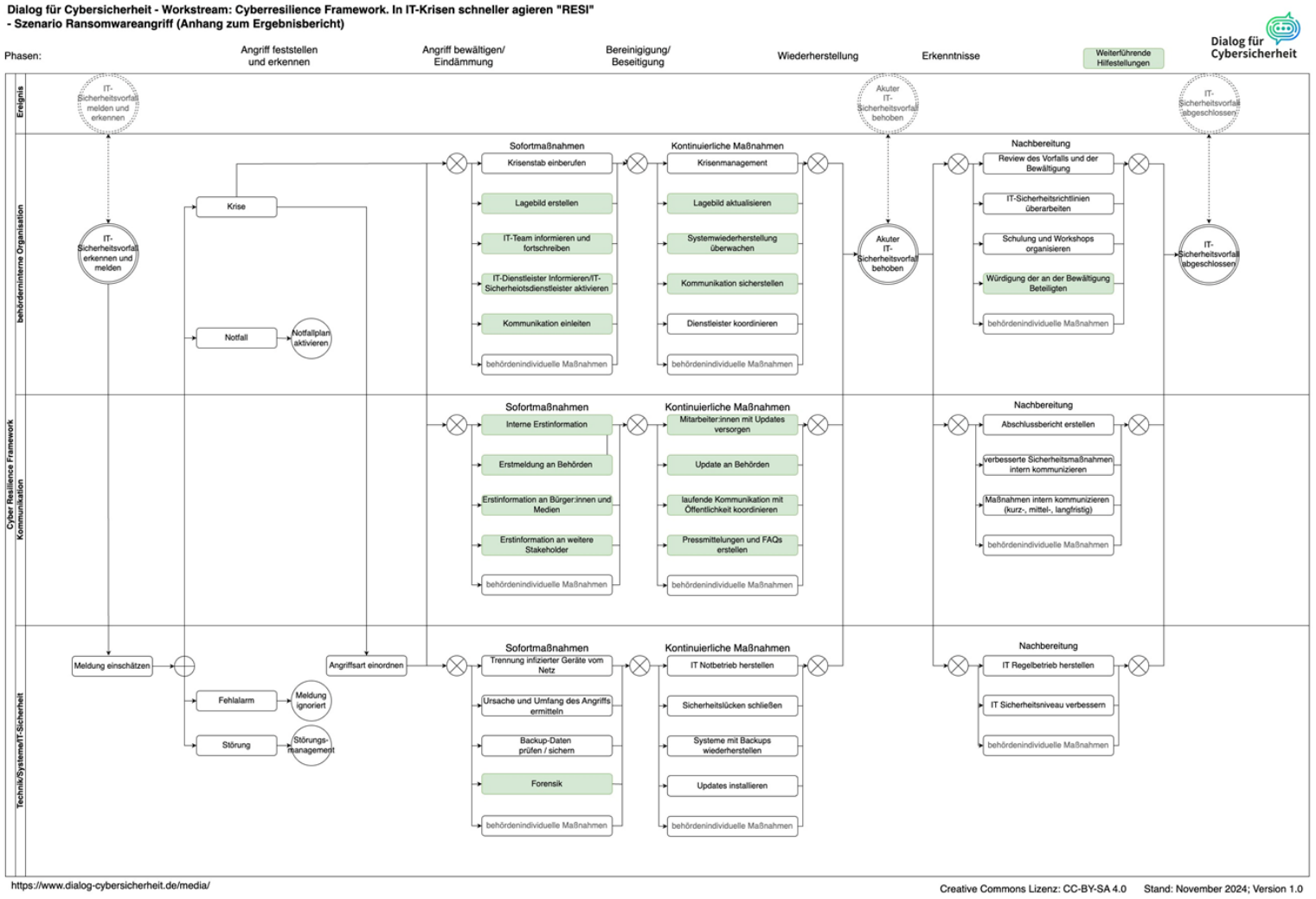
Abgrenzung:

- Störung
- Notfall
- Krise



- Klare Rollen, Kommunikationswege, Entscheidungsprozesse
- Gute Vorbereitung verkürzt Reaktionszeit & minimiert Schaden
- Einheitliche Struktur für Kommunen, Behörden & Dienstleister
- Orientierung auch bei Stress, Unsicherheit & Zeitdruck

Das Szenario – Eine Blaupause für den Ernstfall

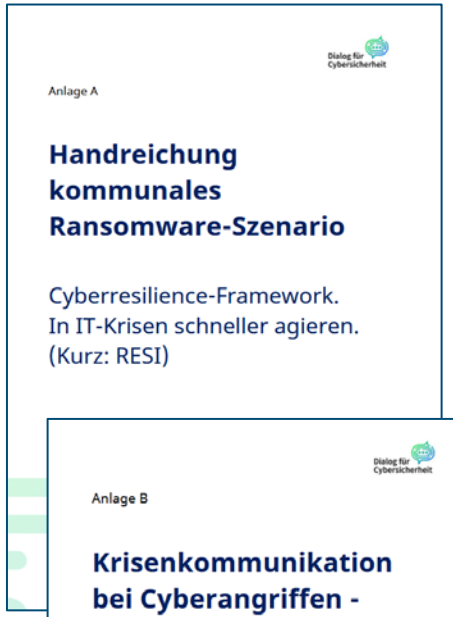


3 Handlungsstränge:

- behördeninterne Organisation
- Kommunikation
- Technik/Systeme/IT-Sicherheit

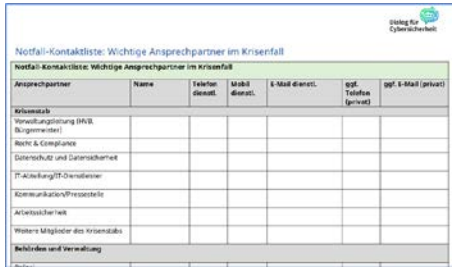
Ergebnisse des Workstreams RESI

Zwei zentrale Handreichungen



- Ablaufdiagramm eines Angriffs mit Phasen & Handlungspfaden
- Verlinkung zu bestehenden & neuen Hilfsmitteln

- Vorlagen, Checklisten, Kontaktlisten
- Unterstützung für interne & externe Kommunikation



Ausblick

- Die Arbeitsgruppe **RESI arbeitet ehrenamtlich weiter**
- Das **Ablaufszenario wurde in ein Prozessmodell nach BPMN** überführt
- **Start mit Szenario-Entwicklung DDoS**
- Aktualisierung des Ergebnisberichtes RESI
- Einarbeitungen von Rückmeldungen – **GERN MITMACHEN**
- Stehen gern als Ansprechpartner zur Verfügung
- E-Mail: resi@dialog-cybersicherheit.de

Laden Sie den RESI Ergebnisbericht hier herunter

Vielen Dank für Ihre Aufmerksamkeit!

Fabienne Tegeler
Fachbereichsleitung „Verbindungswesen und Recht“

Fabienne.Tegeler@bsi.bund.de
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn

www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Follow us: