Cybersicherheitspolitik in Deutschland
Im Fokus Rolle Kommunen

Input beim 8. Kommunaler IT-Sicherheitskongress 2022

04. Mai 2022
Julia Schuetze, Jr. Projektleiterin
Internationale Cybersicherheitspolitik
Stiftung Neue Verantwortung e.V.

Themen

Gefährdungslage: Auswirkungen auf Kommunen

Cybersicherheitsarchitektur: Rollen von Kommunen

Denkanstoß: Cybersicherheitspolitik-Übungen

Austausch

Auswirkungen auf Städte/Kommunen

In den vergangenen Jahren kam es vermehrt zu Cyber-Vorfällen, zum Beispiel Ransomware-Angriffen, bei denen die kommunale Verwaltung in Deutschland selbst betroffen (z. B. Landkreis Anhalt-Bitterfeld (2021), Stadt Witten (2021), Schriesheim (2022)) war oder eine Rolle bei der (Organisation der) Vorfallsbearbeitung gespielt haben (z. B. Stadtwerke Wismar (2021)).

ALLE DATEN VERSCHLÜSSELT

Hackerangriff legt Landkreisverwaltung von Anhalt-Bitterfeld lahm

von MDR SACHSEN-ANHALT
Stand: 07. Juli 2021, 16:46 Uhr

Hackerangriff auf die Stadtverwaltung Witten: Daten erbeutet und veröffentlicht

Am Sonntag, 17. Oktober 2021, ist die Stadt Witten in den frühen Morgenstunden Opfer eines großangelegten Hackerangriffs geworden.

Stadtwerke Wismar: Ermittlungen nach Cyberattacke laufen

Stand: 01.10.2021 17:22 Uhr

Cyberkriminelle haben am Dienstag die IT-Systeme der Stadtwerke in Wismar attackiert. Das wurde am Donnerstag bei der Sitzung der Bürgerschaft bekannt. IT-Sicherheitsexperten arbeiten an der Aufklärung.

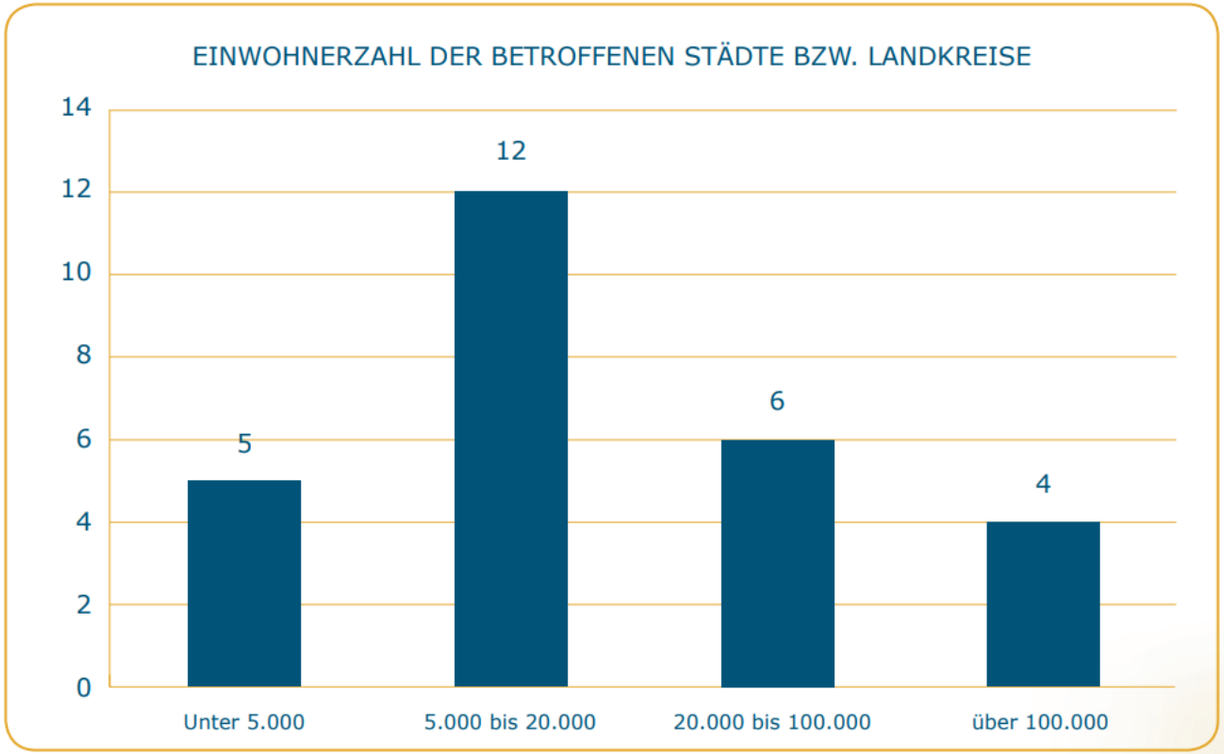
Schriesheim

Verdacht auf Hackerangriff aufs Rathaus hat sich bestätigt

Die "Hacker" drohten der Stadt mit der Veröffentlichung von Daten und stellten ein Ultimatum, ohne aber explizite Geldforderungen zu stellen.

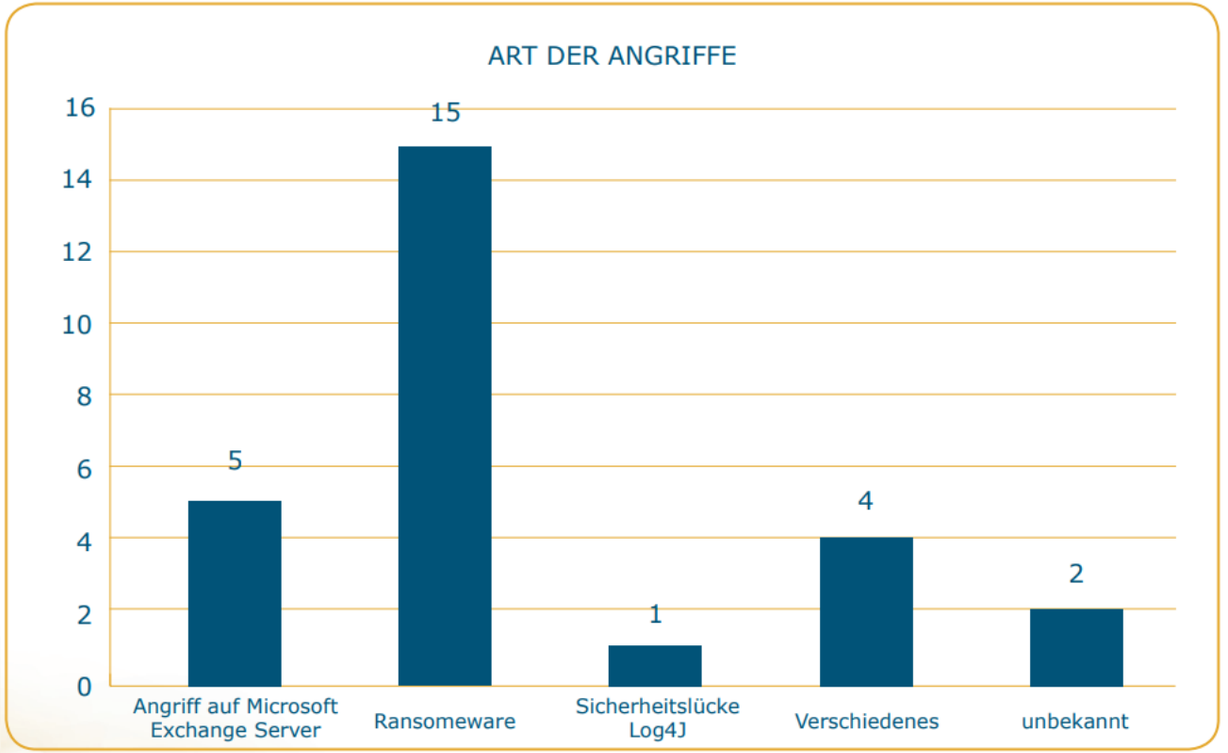
Auswirkungen auf Städte/Kommunen

Abbildung 1: Einwohnerzahl der betroffenen Städte bzw. Landkreise



Quelle: Eigene Darstellung.[9]

Abbildung 2: Art der Angriffe auf kommunale Verwaltungen in Deutschland 2021



Quelle: Eigene Darstellung.

Darstellungen aus Studie von Esther Kern (2022) „Cyberangriffe auf deutsche Kommunen im Jahr 2021“, BIGS Essenz Nummer 19.

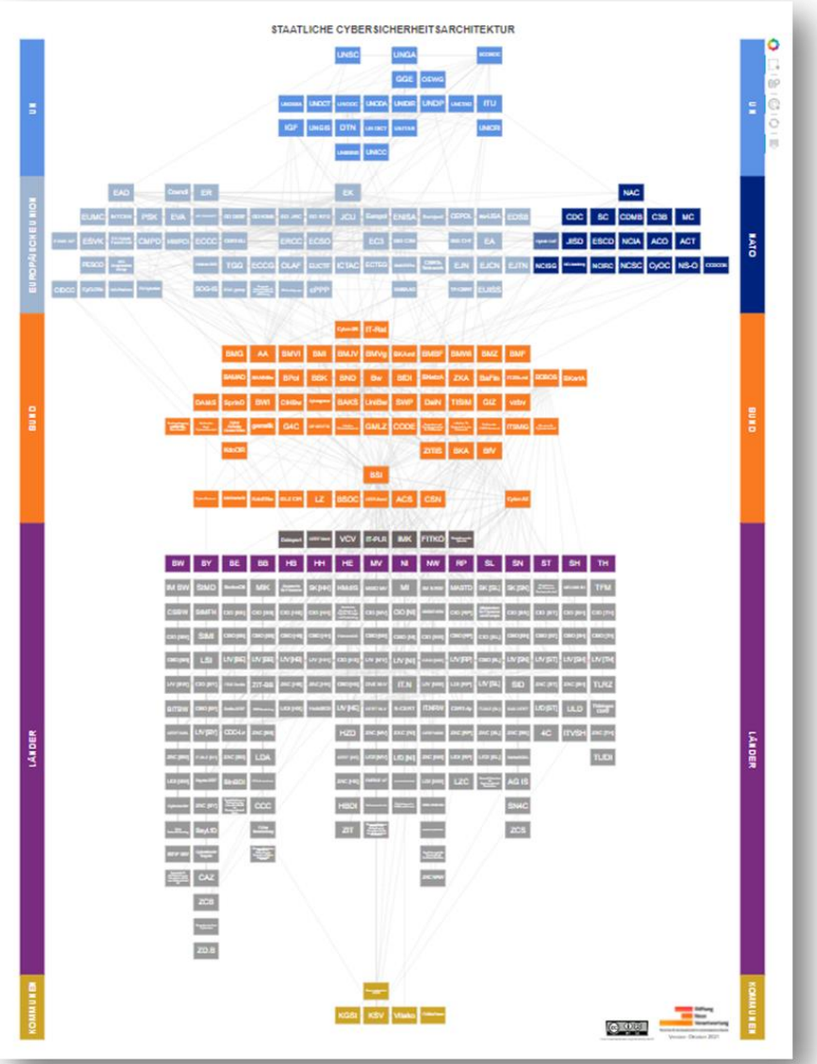
Deutschlands Cybersicherheitsarchitektur

Ausgewählte Akteure Bund

- Bundesamt für Sicherheit in der Informationstechnik
- Nationaler Cybersicherheitsrat
- Nationales Cyber-Abwehrzentrum
- Bundeswehr
- Bundeskriminalamt
- Bundesverfassungsschutz
- IT-Planungsrat
    - FITKO (Föderale IT-Kooperation)

Ausgewählte Akteure Land

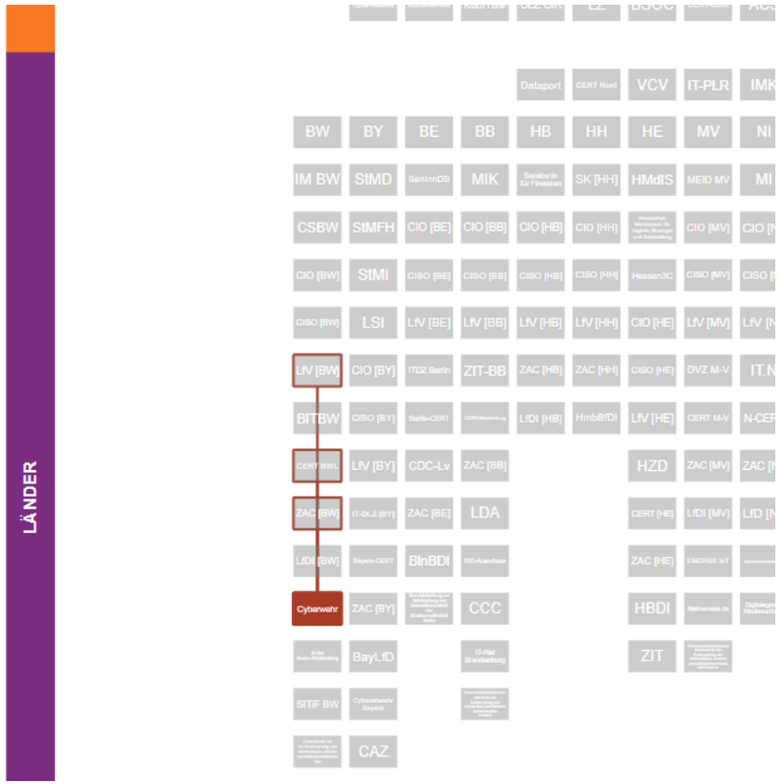
- Ministeriale Zuständigkeit(en) für Themen der Cyber- und IT-Sicherheit (verschieden angesiedelt)
- Landes-CISOs
- Eigene CERTs
- IT-Dienstleister
- Landesverfassungsschutzbehörde
- ZAC Cybercrime
- Kompetenzzentren



Beispiele Länder-Kommunen-Zusammenarbeit

Beispiele Länder-Kommunen-Zusammenarbeit

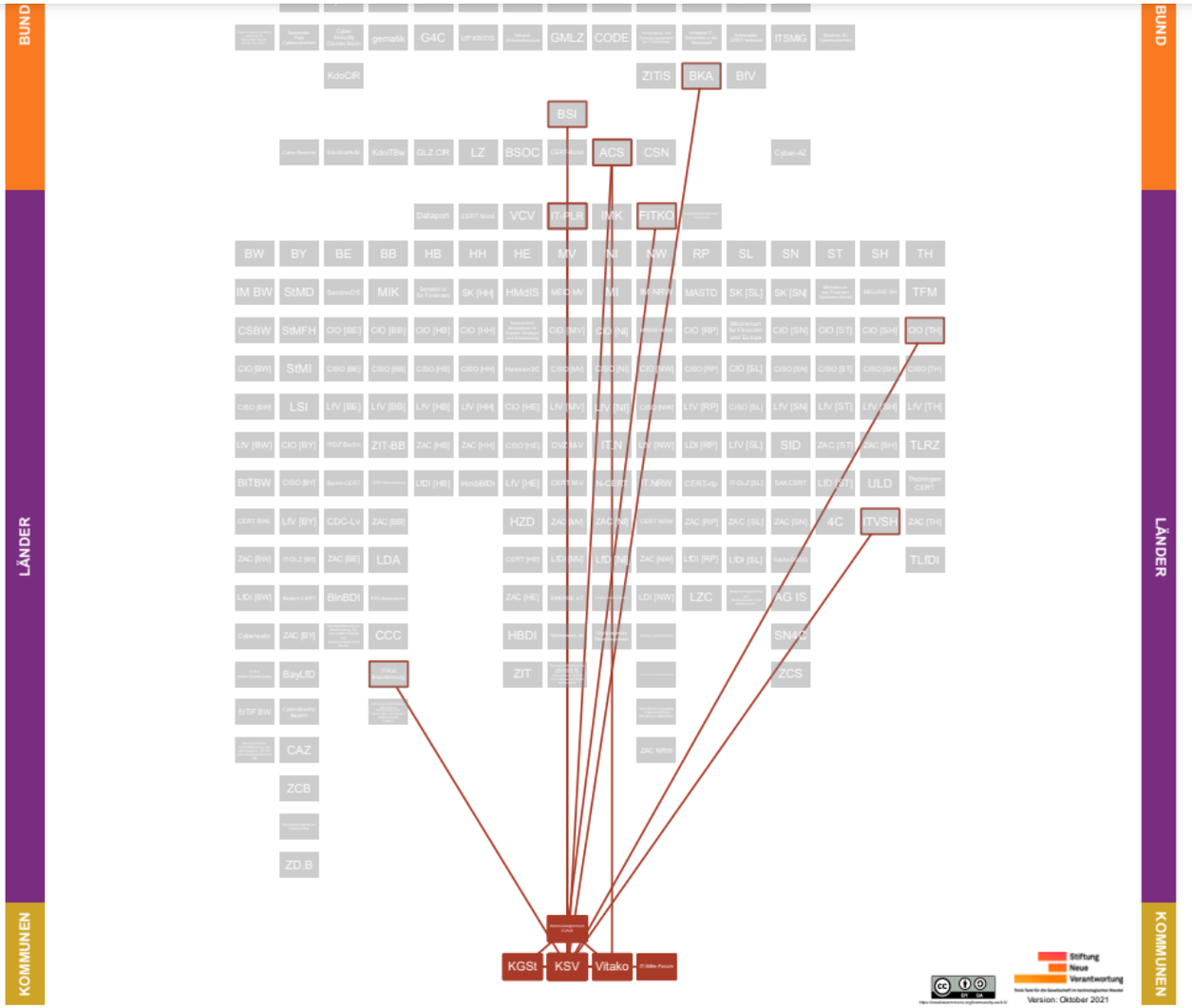
- Cyberhilfswerk (Konzeptidee) (Sachsen-Anhalt)
- Cyberwehr (Baden-Württemberg)
- Kommunal-CERT (NRW)
- CERT-rlp (Rheinland-Pfalz)
- N-CERT (Niedersachsen)
- Implementierung eines Informationssicherheits-Managementsystems bei kommunalen Gebietskörperschaften (ISMS-Förderrichtlinie) (Bayern)



Beispiele: Kommunale IT-Sicherheitsakteure

Kommunale Akteure

- Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister (Vitako)
- IT-SiBe-Forum
- Kommunale Gemeinschaftsstelle für Verwaltungsmanagement (KGSt)
- Kommunale Spitzenverbände (KSV)
- Kommunalgremium des IT-Planungsrates



Rolle von Städten/Kommunalen Akteuren

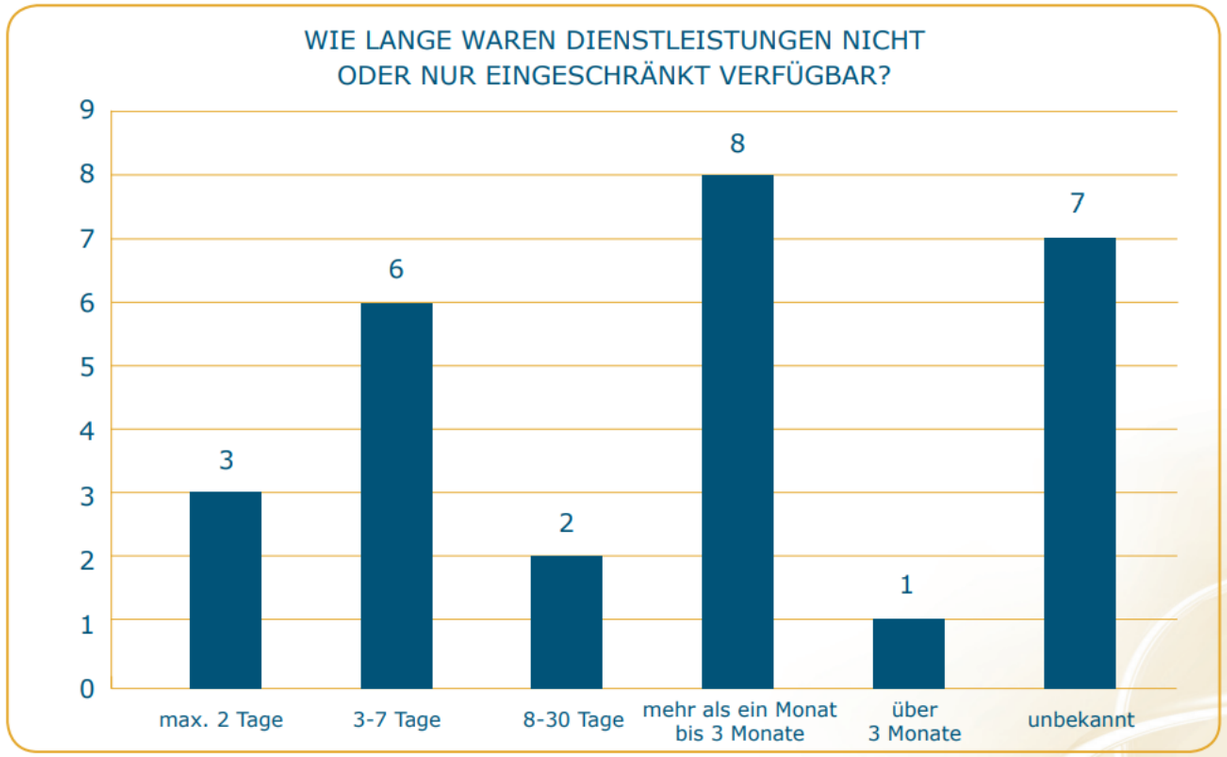
- **Absicherung** der IT-Dienstleistungen
- **Austausch** über Best Practices und pol. Modelle
- **Detektion/(freiwillige) Meldung von Vorfällen**
- **Vorfallsbearbeitung** z.B. Kommunikation, Koordination, Wiederherstellung der Versorgung und IT-Dienstleistungen nach einem Vorfall ermöglichen

Orientierung an: IT-Grundschutzprofil Basisabsicherung Kommunalverwaltung und Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung

„Die Leitlinie für die Informationssicherheit gilt nach Verabschiedung durch den IT-PLR für alle Behörden und Einrichtungen der Verwaltungen des Bundes und der Länder. Den Kommunen, den Verwaltungen des Deutschen Bundestages und der Landesparlamente, den Rechnungshöfen von Bund und Ländern sowie sonstigen Einrichtungen der öffentlichen Verwaltung wird die Anwendung der Leitlinie für die Informationssicherheit empfohlen."

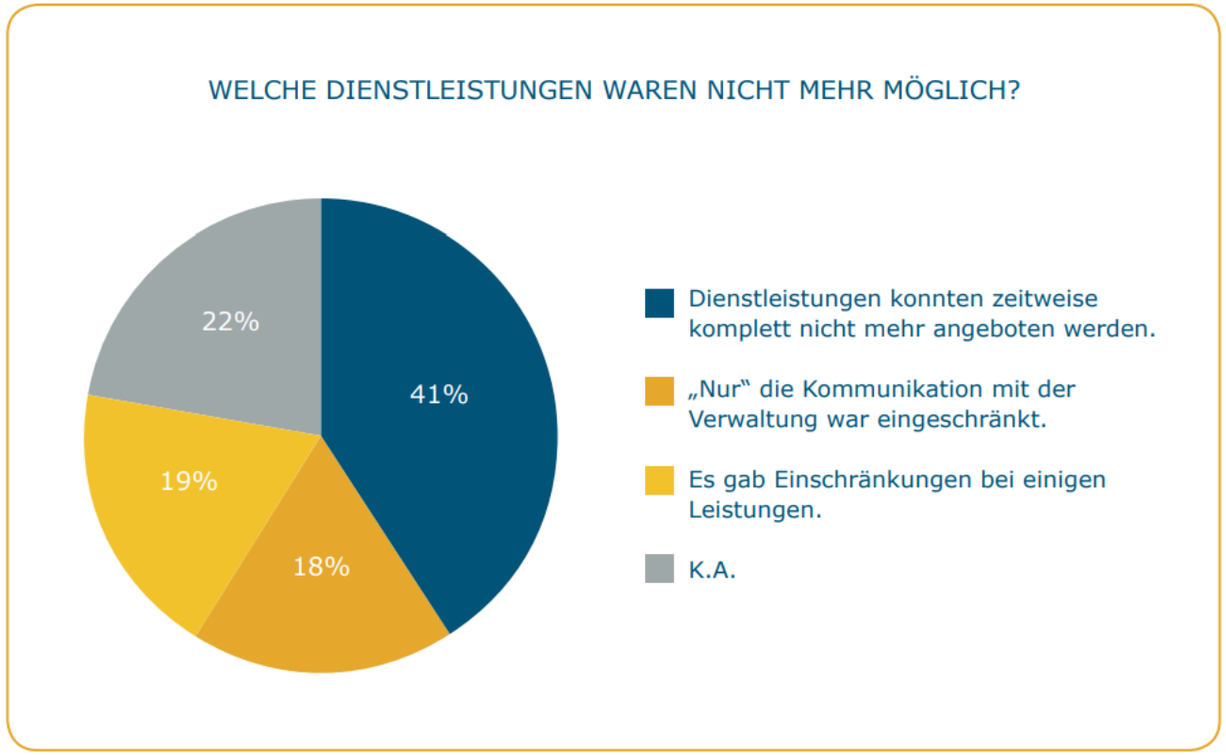
Fokus Vorfallsbearbeitung: Wie wird reagiert? Wie wird der Schaden minimiert?

Abbildung 3: Zeitraum, in dem Verwaltungen ihre Dienstleistungen nicht oder nur eingeschränkt anbieten konnten



Quelle: Eigene Darstellung.[23]

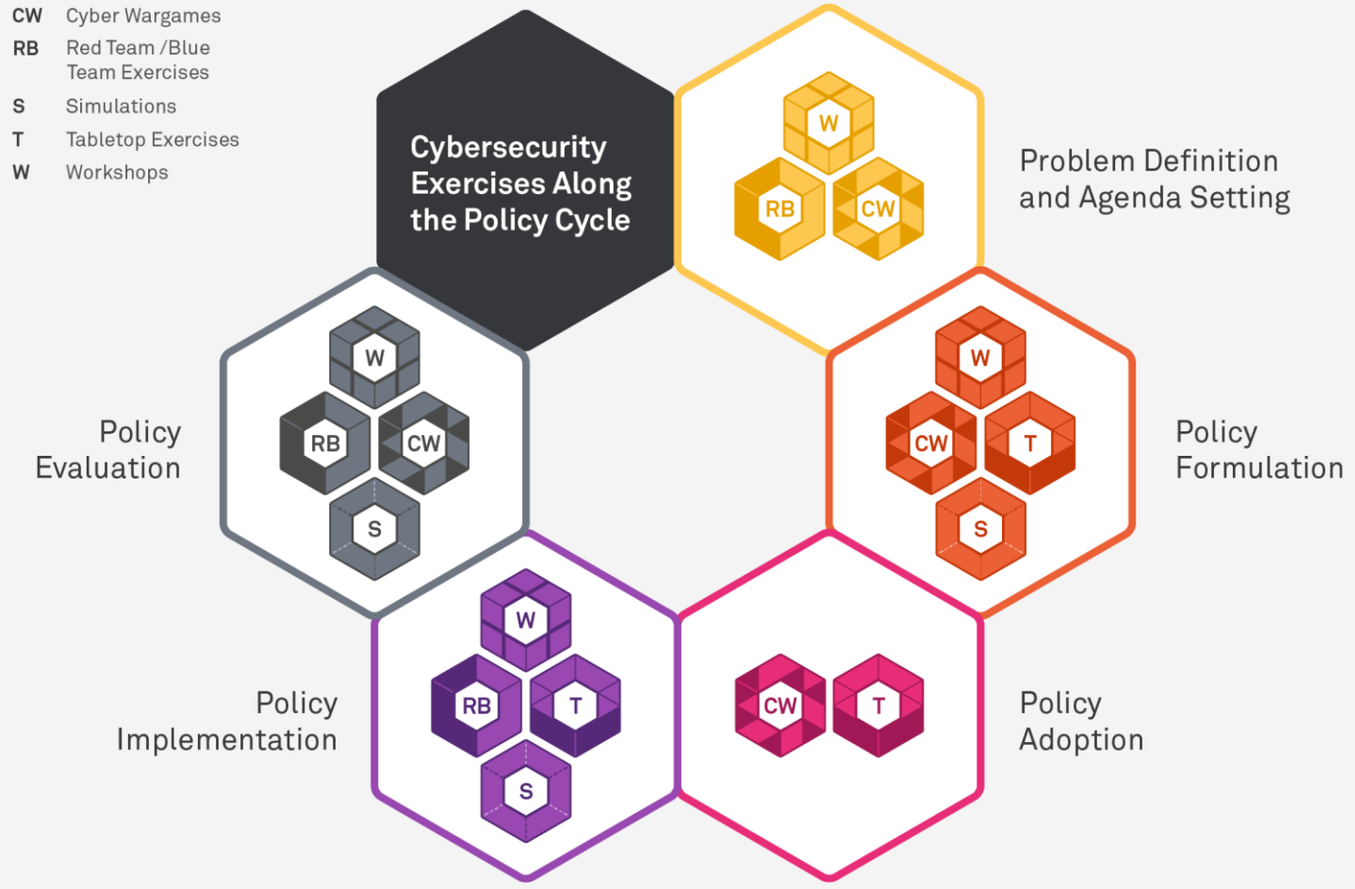
Abbildung 4: Welche Dienstleistungen waren eingeschränkt?



Quelle: Eigene Darstellung.

Darstellungen aus Studie von Esther Kern (2022) „Cyberangriffe auf deutsche Kommunen im Jahr 2021“, BIGS Essenz Nummer 19.

Cybersicherheitsübungen zur Vorbereitung



Darstellung aus Studie von Beigel & Schuetze (2021) „Cybersecurity Exercises for Policy Work“, SNV.

Mögliche Ziele einer Table-Top während Policy Implementierungs-Phase

1) Verbessertes Verständnis der gesetzlichen/organisatorischen Anforderungen und implementierten Richtlinien
2) Verbesserung der Zusammenarbeit zwischen den Akteuren/Sektoren (nationale Ebene)
3) Üben des Austauschs von Informationen und Analysen zwischen verschiedenen Institutionen
4) Praxisbewertung und Analyse von Vorfällen
5) Praktizieren der Maßnahmen der öffentlichen Kommunikation
6) Kooperationsmaßnahmen zwischen nationalen und internationalen Akteuren identifizieren (internationale Ebene)
7) Klärung der Verantwortlichkeiten von Institutionen/Personen
8) Entwicklung von Verbesserungsmöglichkeiten/Notfallprozessen

Quelle: Stiftung Neue Verantwortung e.V.

Gruppenaufgabe “Meldung eines Cybervorfalls”

Bisher sind die meisten Kommunen davon ausgenommen Vorfälle an Bundes- oder Landesbehörden zu melden.

Wie würde ein idealer Meldungsprozess aussehen? Wer würde benachrichtigt werden? Und würde diese Stelle die Information weiterleiten? Welche Erwartungen gibt es an einen Meldungsprozess?

Quelle: Stiftung Neue Verantwortung e.V.

Besten Dank!
Ich freue mich auf Austausch/Rückmeldungen.

Julia Schuetze
Jr. Projektleiterin
Internationale Cybersicherheitspolitik
Stiftung Neue Verantwortung e.V.
jschuetze@stiftung-nv.de
@juschuetze bei Twitter