CSBW

CYBER
SICHERHEITS
AGENTUR
BADEN-WÜRTTEMBERG

Von IT-Notfallübungen über Notfallequipment bis zum Cybervorfall Best Practice

Dominik Schuler, Stab der CSBW

06.05.2025

Baden-Württemberg

11.339 mio. (2023)

BIP 615 mrd. € p.a. (2023)

Innovationsführer in Europa (2022)

(Vgl. zu Schweden)

Höchste Dichte an globalen Weltmarktführern & KMU, insb. Hidden Champions in Europa

Was ist die Cybersicherheitsagentur BW?

Kurz: CSBW

Die CSBW ist eine **Landesoberbehörde** in Baden-Württemberg.
Gegründet im Jahr 2021 auf Grundlage des Cybersicherheitsgesetzes, ist sie seit dem 1. Januar 2022 eigenständig.

Die CSBW ist zentrale Melde- und Koordinierungsstelle für Cybersicherheitsvorfälle im Land. Ihre Aufgabe ist die **Verbesserung der Cybersicherheit in Baden-Württemberg**.

Die CSBW verfolgt einen 360-Grad-Ansatz für die Cybersicherheit.
Sie ist in den Bereichen **Prävention, Detektion und Reaktion** tätig.

Cybersicherheitsarchitektur Baden-Württemberg

CSBW

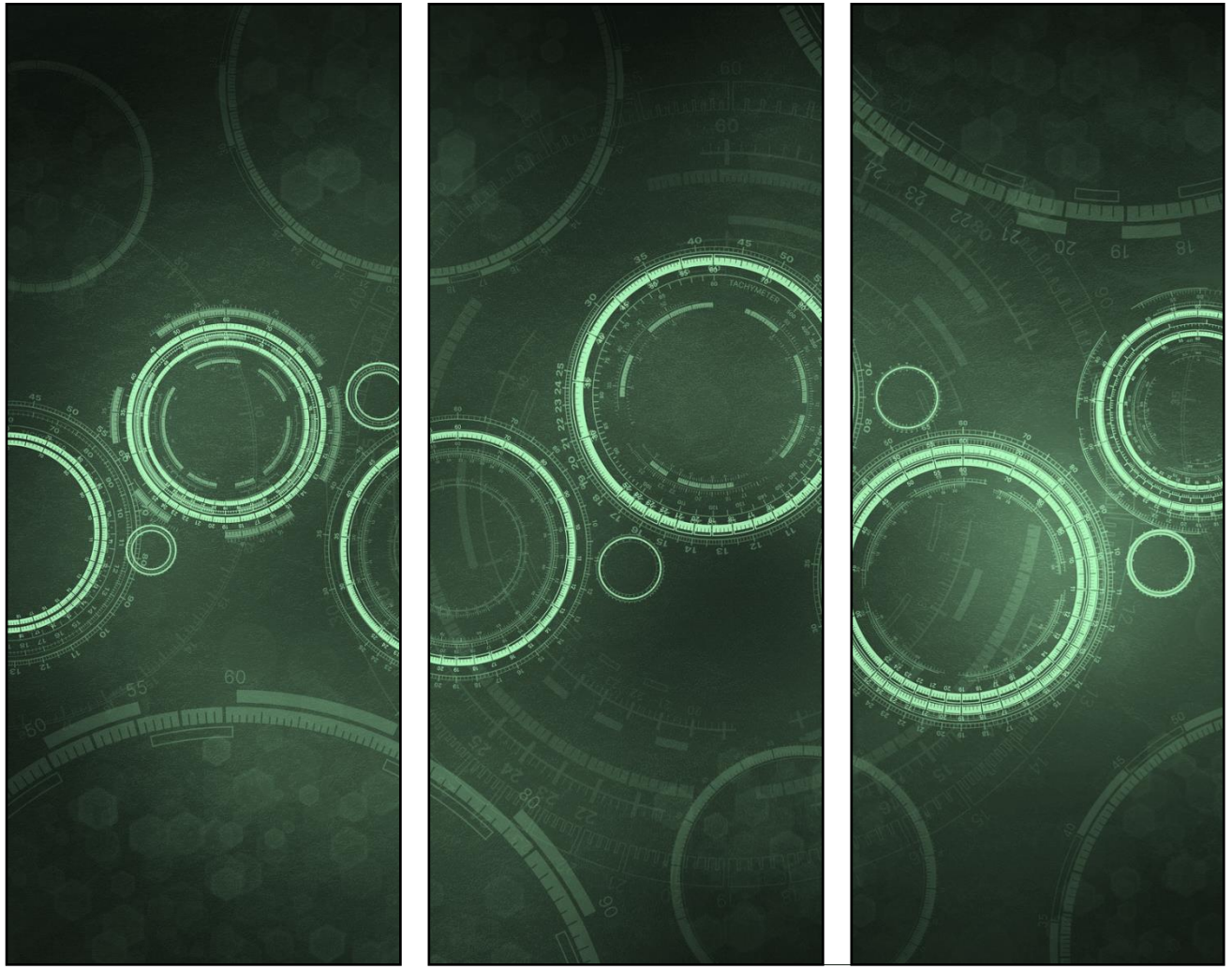
als Teil der gesamtstaatlichen Cybersicherheitsarchitektur

88,5 FTE

Prävention
Detektion
Reaktion

Cybersicherheitsgesetz Baden-Württemberg (2021)

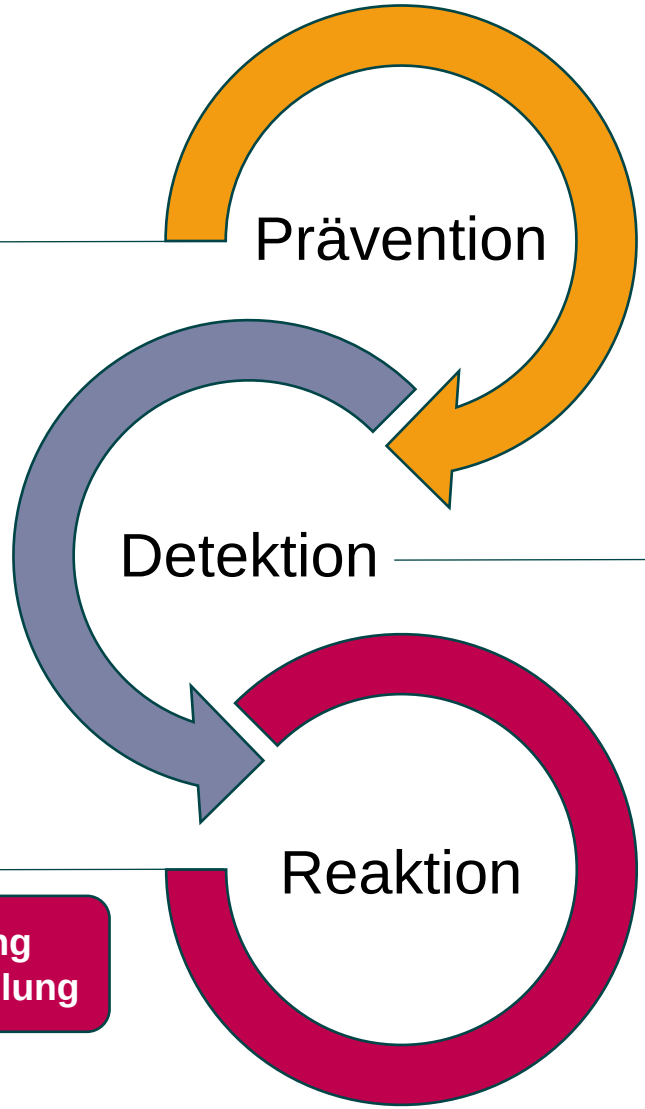
Enge Partnerschaft mit LKA, LfV, BSI und internationalen Partnern



Der 360° Ansatz der CSBW

Schulung- und Sensibilisierung

Beratung zu Schutzmaßnahmen



Warn- und Informationsdienst

Unterstützung Cybersicherheitsvorfall

Krisen-management

Techn. Analyse

Vorbereitung Wiederherstellung

Präventionsaspekte

Basisportfolio Prävention

Hochschulen

KMU

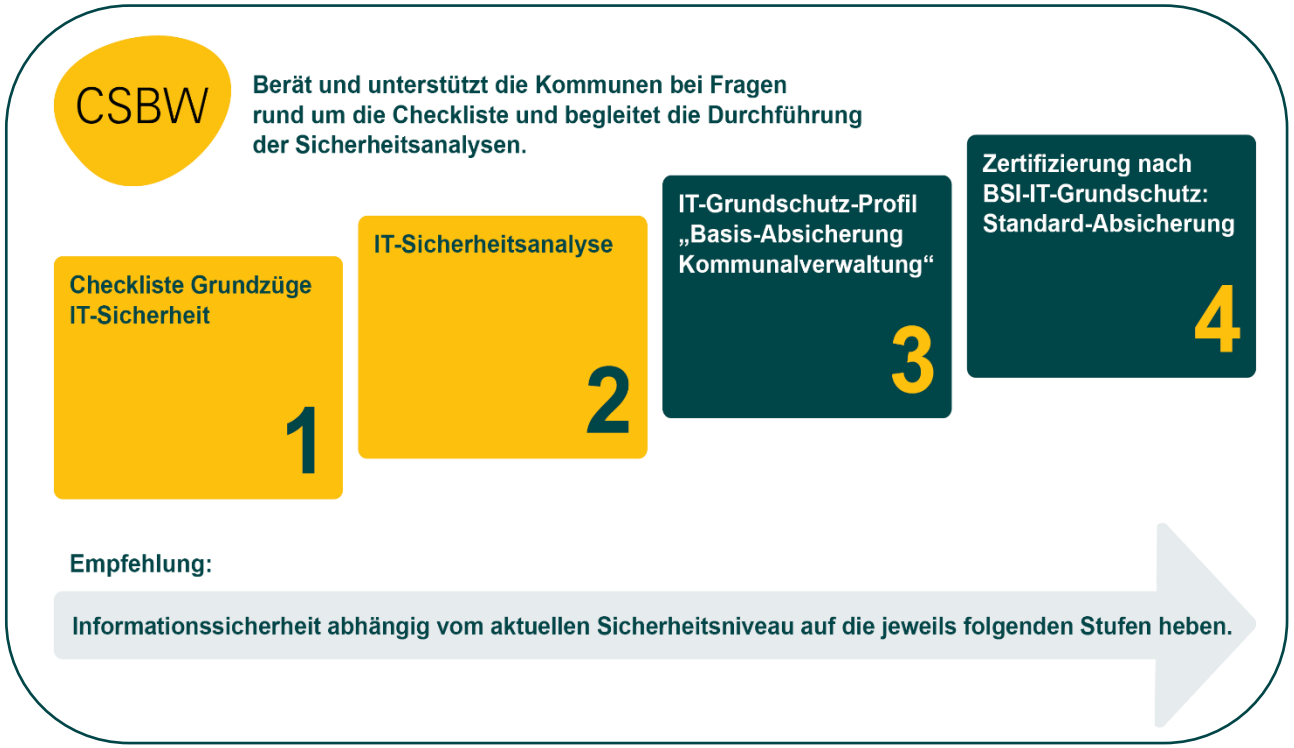
Kommunen

Beratungsangebote

Schulungen

Factsheets

Erklärvideos

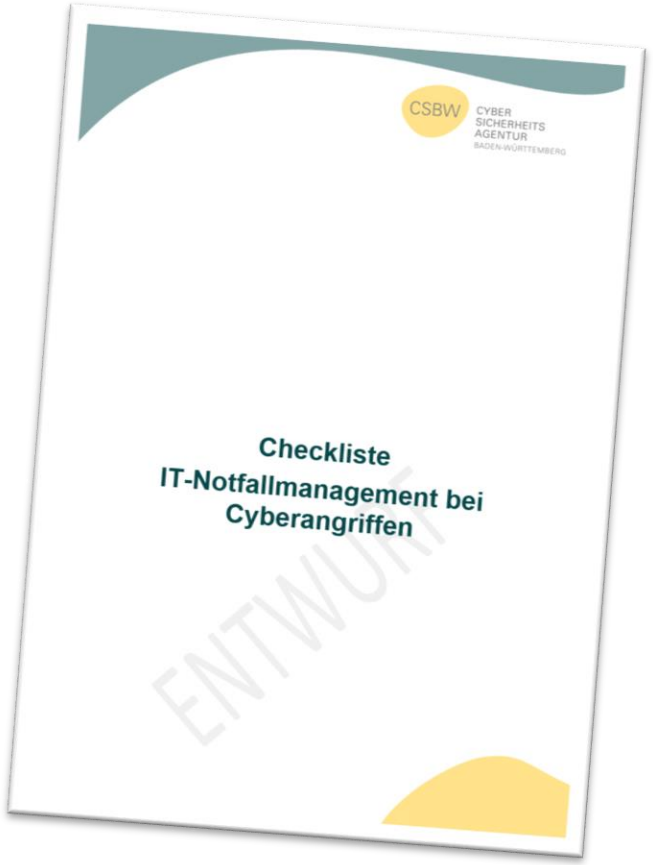


ISMS-Vorlagen

Aus den Vorfällen lernen, Erkenntnisse dokumentieren & Wissen verfügbar machen

Aktuell bereits verfügbare Dokumente

- Leitlinie zur Informationssicherheit
- IT-Nutzungsrichtlinie
- Bestellungsurkunde einer oder eines ISB
- IT-Betriebshandbuch
- Berechtigungskonzept
- Checkliste IT-Notfallmanagement bei Cyberangriffen



E-Mail an beratung@cybersicherheit.bwl.de Stichwort „ISMS-Vorlagen“

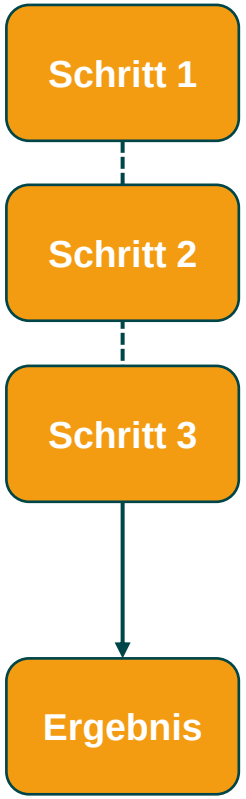
Pilotprojekt IT-Notfallübung

Start Herbst 2024

5 Pilotkommunen

Realitätsnahes Szenario testen

Ziel Konzept für IT-Notfallübungen

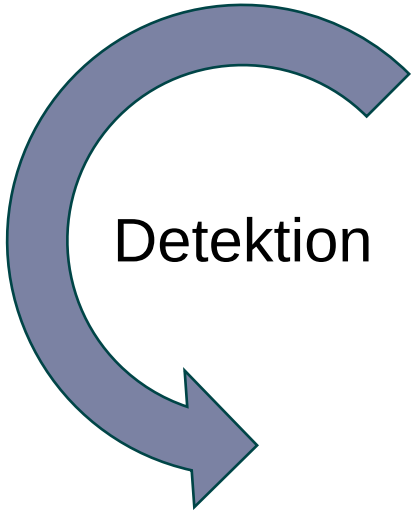


Feststellung des Sicherheitsniveaus sowie der individuellen Anforderungen der Organisation

Durchführung vor Ort (Cyber-Simulation, Wissenstransfer Krisenmanagement, Umsetzung Bedarfe in Kleingruppen)

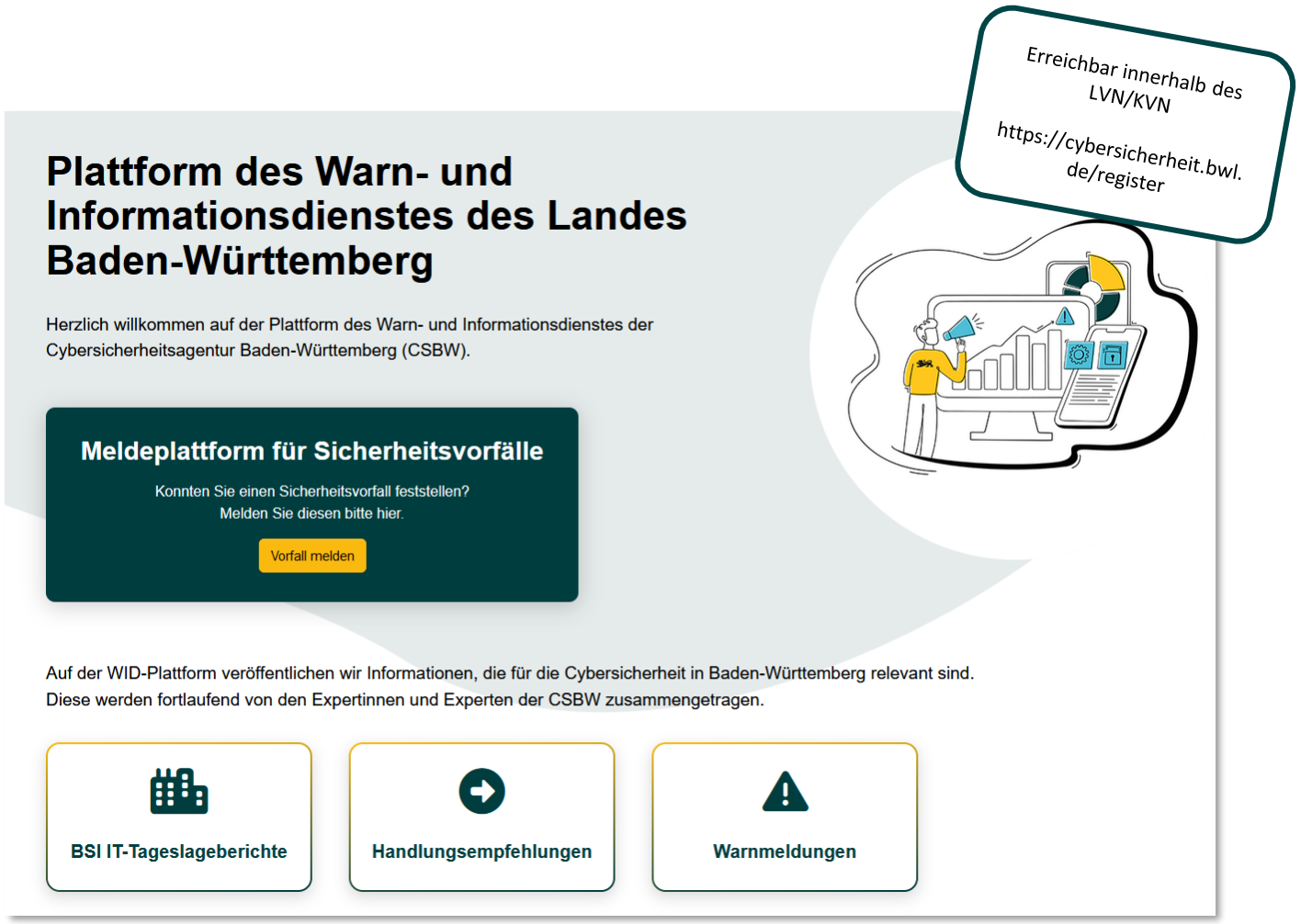
Dokumentation und individuelle Handlungsempfehlung

IT-Notfallübungen als ständiges Angebot der CSBW für alle Kommunen

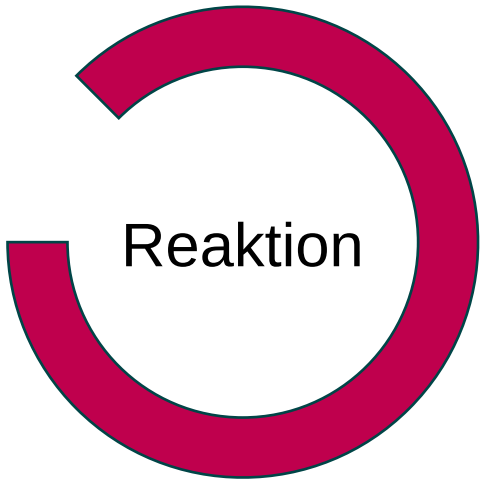


Warn- und Informationsdienste

Informationsprodukte des WID



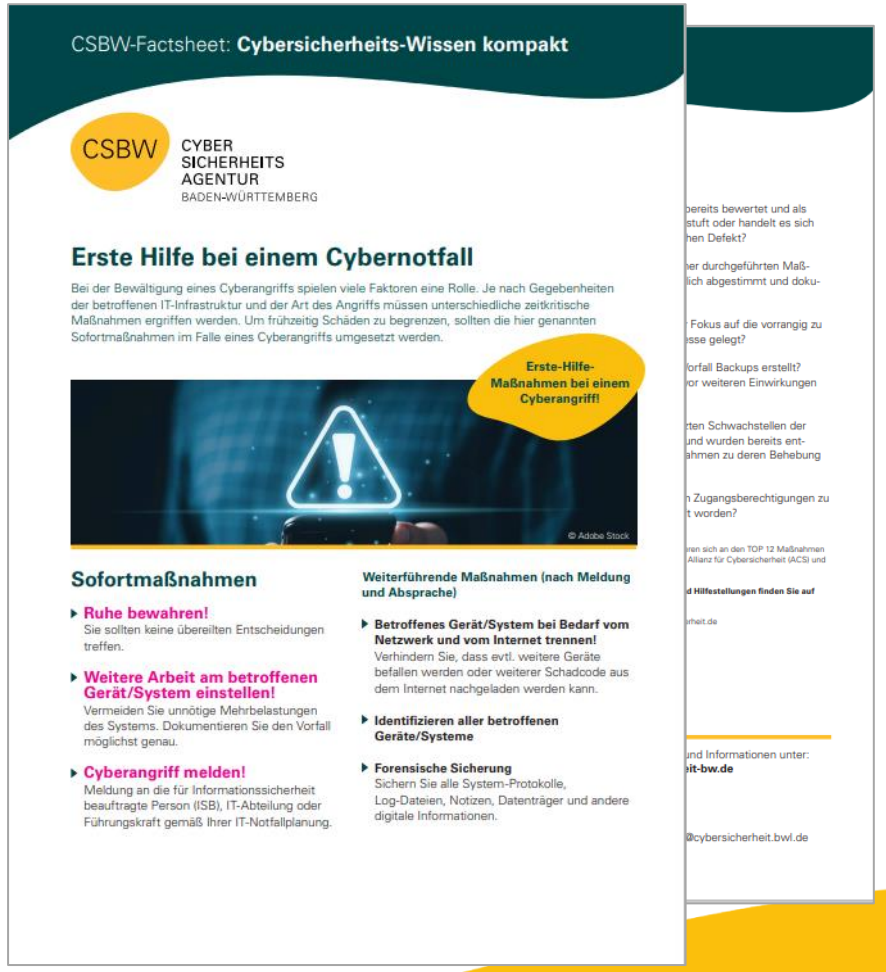
- **CSBW-Warnmeldungen:**
  Warnmeldungen der CSBW vor konkreten, aktuellen Gefahren, Schwachstellen oder Kampagnen
- **CSBW-Handlungsempfehlungen:**
  Handlungsempfehlungen der CSBW zu allgemeinen Gefahren
- **BSI IT-Tageslagebericht:**
  IT-Tageslagebericht des BSI
- **BSI IT-Sicherheitswarnung:**
  IT-Sicherheitswarnungen des BSI



Wenn der Ernstfall eintritt

Sicherheitsvorfall – was soll ich tun?

- Bewahren Sie Ruhe und handeln Sie nicht übereilt.
- Stellen Sie die Arbeit am betroffenen Gerät/System ein.
- Melden Sie den Vorfall. Wissen alle davon, die davon wissen müssen?
- Trennen Sie das Gerät von internen Netzwerken und dem Internet (Kabel und WLAN).
- Gerät nicht herunterfahren oder ausschalten.
- Machen Sie sich Notizen zu Zeitpunkt, Auffälligkeiten, Aktivitäten etc.



CSBW-Factsheet: **Cybersicherheits-Wissen kompakt**

CSBW CYBER SICHERHEITS AGENTUR BADEN-WÜRTTEMBERG

Erste Hilfe bei einem Cybernotfall

Bei der Bewältigung eines Cyberangriffs spielen viele Faktoren eine Rolle. Je nach Gegebenheiten der betroffenen IT-Infrastruktur und der Art des Angriffs müssen unterschiedliche zeitkritische Maßnahmen ergriffen werden. Um frühzeitig Schäden zu begrenzen, sollten die hier genannten Sofortmaßnahmen im Falle eines Cyberangriffs umgesetzt werden.

Erste-Hilfe-Maßnahmen bei einem Cyberangriff!

© Adobe Stock

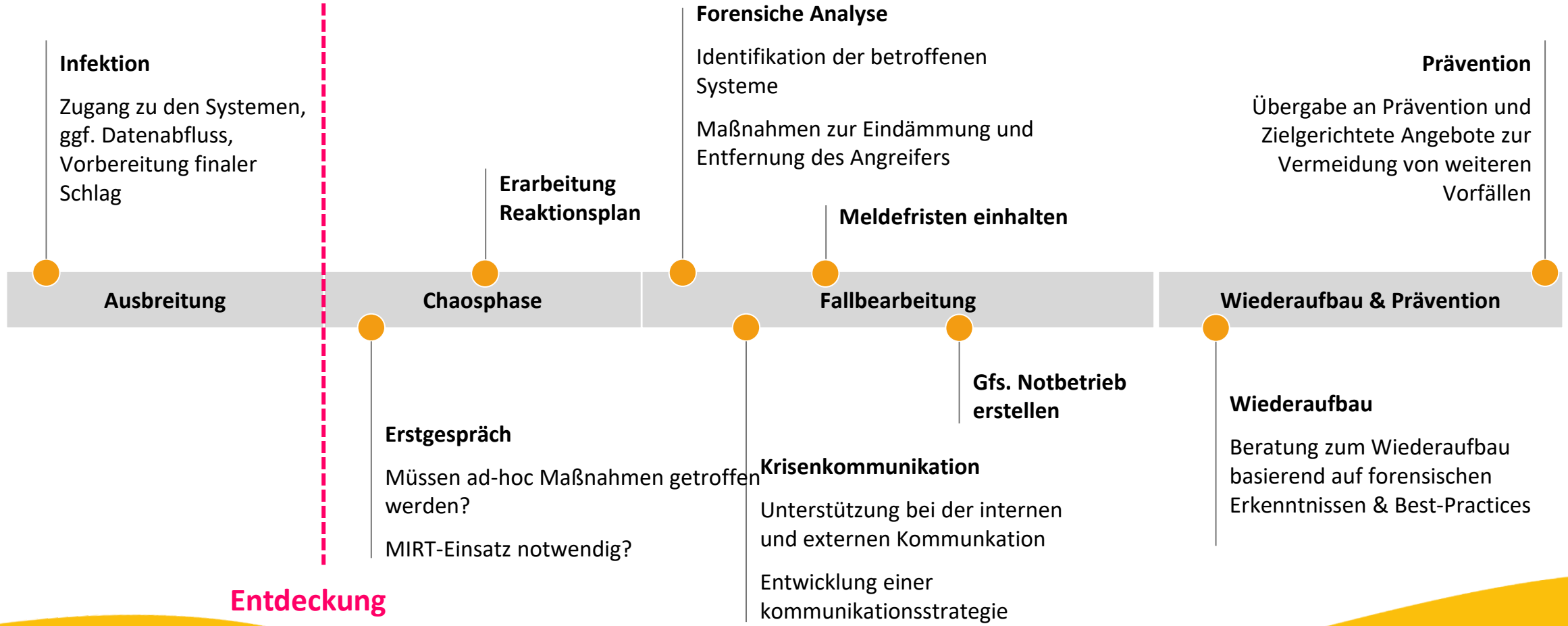
Sofortmaßnahmen

- **Ruhe bewahren!**
  Sie sollten keine übereilten Entscheidungen treffen.
- **Weitere Arbeit am betroffenen Gerät/System einstellen!**
  Vermeiden Sie unnötige Mehrbelastungen des Systems. Dokumentieren Sie den Vorfall möglichst genau.
- **Cyberangriff melden!**
  Meldung an die für Informationssicherheit beauftragte Person (ISB), IT-Abteilung oder Führungskraft gemäß Ihrer IT-Notfallplanung.

Weiterführende Maßnahmen (nach Meldung und Absprache)

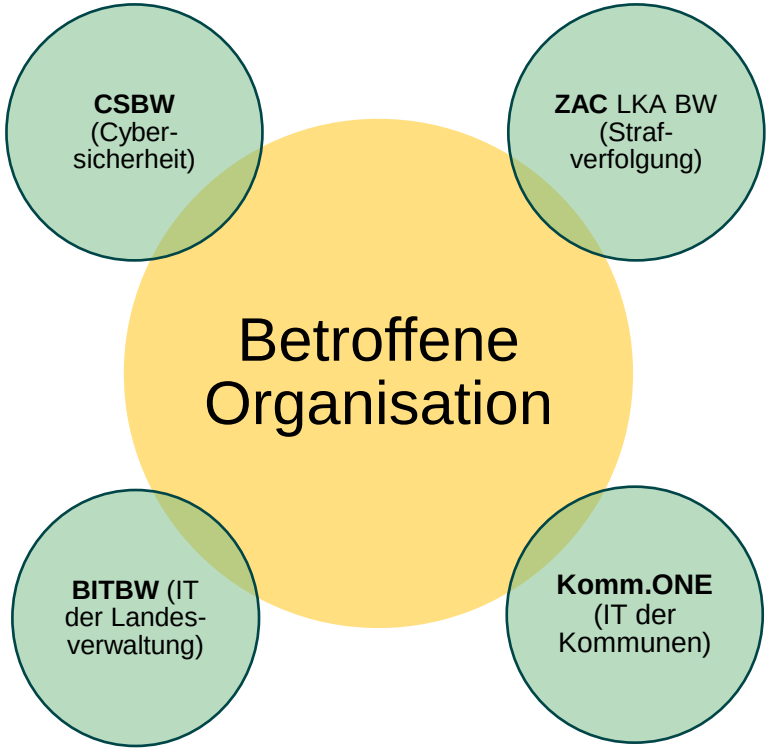
- **Betroffenes Gerät/System bei Bedarf vom Netzwerk und vom Internet trennen!**
  Verhindern Sie, dass evtl. weitere Geräte befallen werden oder weiterer Schadcode aus dem Internet nachgeladen werden kann.
- **Identifizieren aller betroffenen Geräte/Systeme**
- **Forensische Sicherung**
  Sichern Sie alle System-Protokolle, Log-Dateien, Notizen, Datenträger und andere digitale Informationen.

Die Phasen eines Sicherheitsvorfalls - Überblick



IT-Sicherheitsvorfälle bearbeiten wir gemeinsam

Nur **gemeinsam** können IT-Sicherheitsvorfälle vollumfänglich und ergebnisorientiert bearbeitet werden!

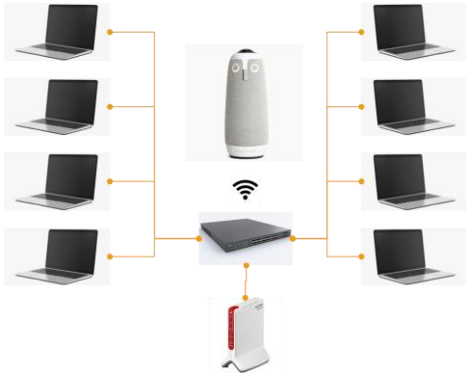


- **Regelmäßiger Austausch** zwischen BITBW, ZAC, LfV, Komm.ONE und CSBW
- **Anlassbezogener Austausch**

Notfallequipment

CSBW – “Virtueller Krisenstab”

- ✓ max. 10 Laptops (ohne Zugriff auf das LVN / KVN)
- ✓ Switch & Verkabelung
- ✓ mobiler Router inkl. Internetanbindung
- ✓ Videokonferenzsystem



Komm.ONE

Coming soon

Kommunikationsfähigkeit des Krisenstabs sicherstellen

Arbeitsfähigkeit der Verwaltung wiederherstellen

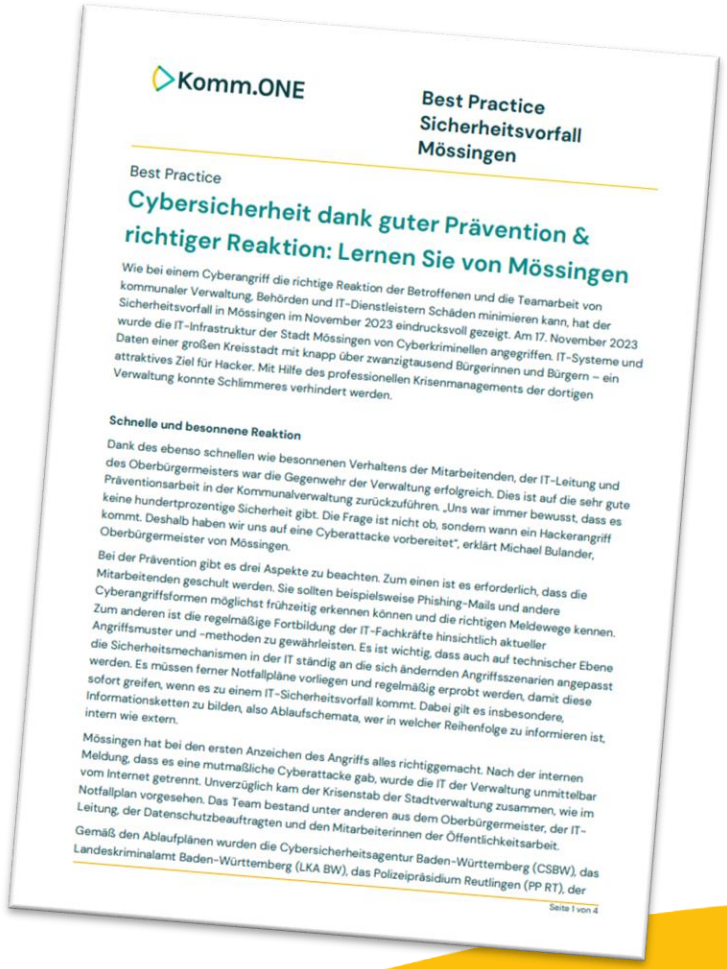
Best Practice Mössingen

Wichtige Erkenntnisse:

- Schnelle und besonnene Reaktion.
- Akribische Forensik und abgestimmte Kommunikation.
- Sicherer und sorgfältiger Wiederaufbau.
- Optimiert in die Zukunft dank kritischem Rückblick.

Vollständiger Bericht unter

https://www.cybersicherheit-bw.de/aktuelles/best-practice-moessingen



Komm.ONE

Best Practice
Sicherheitsvorfall
Mössingen

Best Practice

Cybersicherheit dank guter Prävention & richtiger Reaktion: Lernen Sie von Mössingen

Wie bei einem Cyberangriff die richtige Reaktion der Betroffenen und die Teamarbeit von kommunaler Verwaltung, Behörden und IT-Dienstleistern Schäden minimieren kann, hat der Sicherheitsvorfall in Mössingen im November 2023 eindrucksvoll gezeigt. Am 17. November 2023 wurde die IT-Infrastruktur der Stadt Mössingen von Cyberkriminellen angegriffen. IT-Systeme und Daten einer großen Kreisstadt mit knapp über zwanzigtausend Bürgerinnen und Bürgern – ein attraktives Ziel für Hacker. Mit Hilfe des professionellen Krisenmanagements der dortigen Verwaltung konnte Schlimmeres verhindert werden.

Schnelle und besonnene Reaktion

Dank des ebenso schnellen wie besonnenen Verhaltens der Mitarbeitenden, der IT-Leitung und des Oberbürgermeisters war die Gegenwehr der Verwaltung erfolgreich. Dies ist auf die sehr gute Präventionsarbeit in der Kommunalverwaltung zurückzuführen. „Uns war immer bewusst, dass es keine hundertprozentige Sicherheit gibt. Die Frage ist nicht ob, sondern wann ein Hackerangriff kommt. Deshalb haben wir uns auf eine Cyberattacke vorbereitet", erklärt Michael Bulander, Oberbürgermeister von Mössingen.

Bei der Prävention gibt es drei Aspekte zu beachten. Zum einen ist es erforderlich, dass die Mitarbeitenden geschult werden. Sie sollten beispielsweise Phishing-Mails und andere Cyberangriffsformen möglichst frühzeitig erkennen können und die richtigen Meldewege kennen. Zum anderen ist die regelmäßige Fortbildung der IT-Fachkräfte hinsichtlich aktueller Angriffsmuster und -methoden zu gewährleisten. Es ist wichtig, dass auch auf technischer Ebene die Sicherheitsmechanismen in der IT ständig an die sich ändernden Angriffsszenarien angepasst werden. Es müssen ferner Notfallpläne vorliegen und regelmäßig erprobt werden, damit diese sofort greifen, wenn es zu einem IT-Sicherheitsvorfall kommt. Dabei gilt es insbesondere, Informationsketten zu bilden, also Ablaufschemata, wer in welcher Reihenfolge zu informieren ist, intern wie extern.

Mössingen hat bei den ersten Anzeichen des Angriffs alles richtiggemacht. Nach der internen Meldung, dass es eine mutmaßliche Cyberattacke gab, wurde die IT der Verwaltung unmittelbar vom Internet getrennt. Unverzüglich kam der Krisenstab der Stadtverwaltung zusammen, wie im Notfallplan vorgesehen. Das Team bestand unter anderen aus dem Oberbürgermeister, der IT-Leitung, der Datenschutzbeauftragten und den Mitarbeiterinnen der Öffentlichkeitsarbeit.

Gemäß den Ablaufplänen wurden die Cybersicherheitsagentur Baden-Württemberg (CSBW), das Landeskriminalamt Baden-Württemberg (LKA BW), das Polizeipräsidium Reutlingen (PP RT), der

Seite 1 von 4

Vielen Dank!

www.cybersicherheit-bw.de

CSBW