digital@bw
CyberSicherheit

Cybersicherheit für Kommunen

Baden-Württemberg
MINISTERIUM FÜR INNERES, DIGITALISIERUNG UND MIGRATION

23.07.19

digital@bw
CyberSicherheit

Begriff Cyber-Sicherheit

- IT-Sicherheit wird für unsere Gesellschaft, unserer Verwaltung unsere Wirtschaft und Wissenschaft immer wichtiger (Gesundheitskarte, Betreiber von KRITIS, vernetzter Kühlschrank, Smart-City von Morgen, autonomes Fahren etc.)

- aus IT-Sicherheit (Vertraulichkeit, Integrität und Verfügbarkeit von Daten) wird Cyber-Sicherheit in einem ganzheitlichen Sinne.

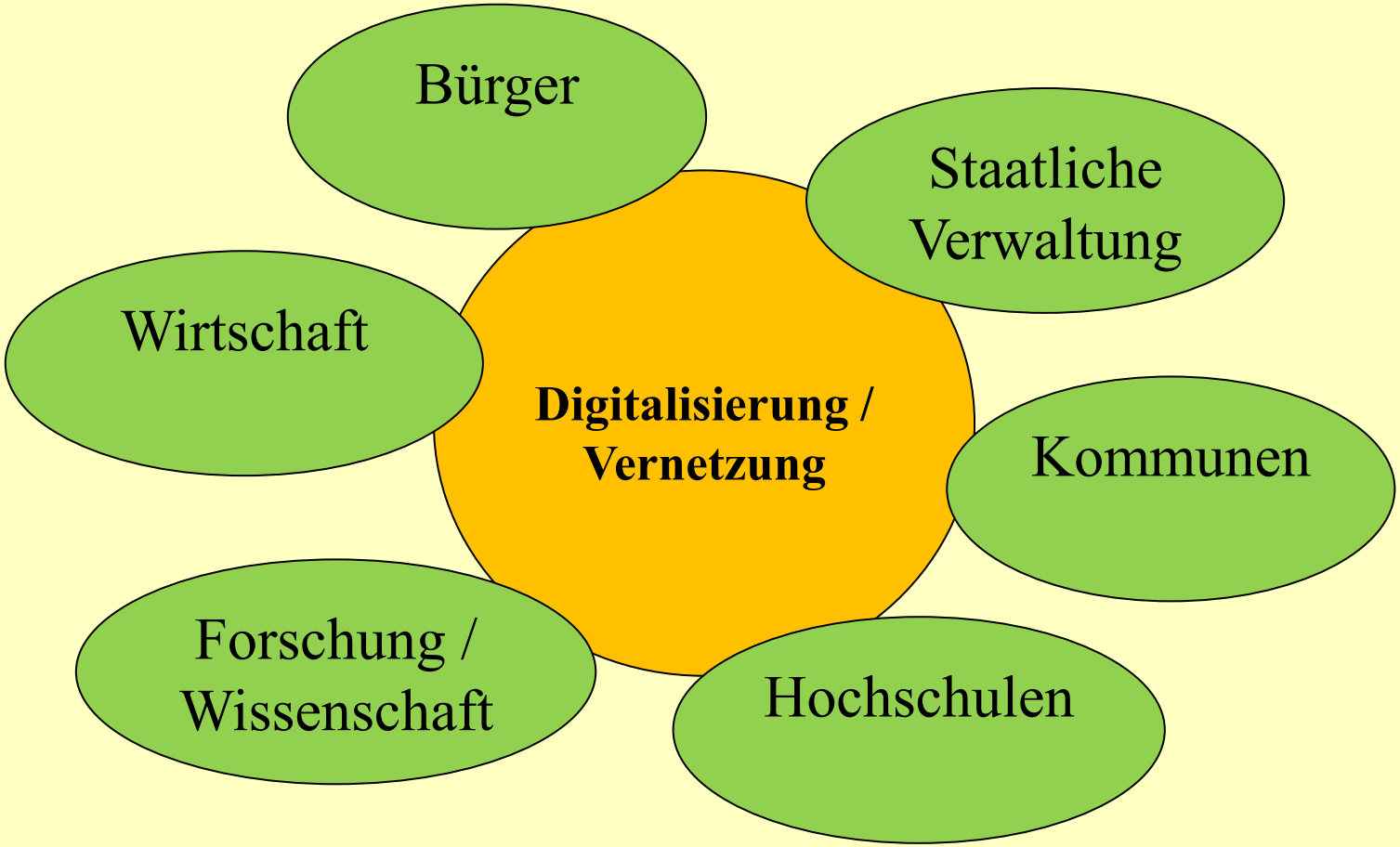
- Cyber-Sicherheit ist also mehr als IT-Sicherheit.

digital@bw CyberSicherheit

Warum ist Cyber-Sicherheit so wichtig ?

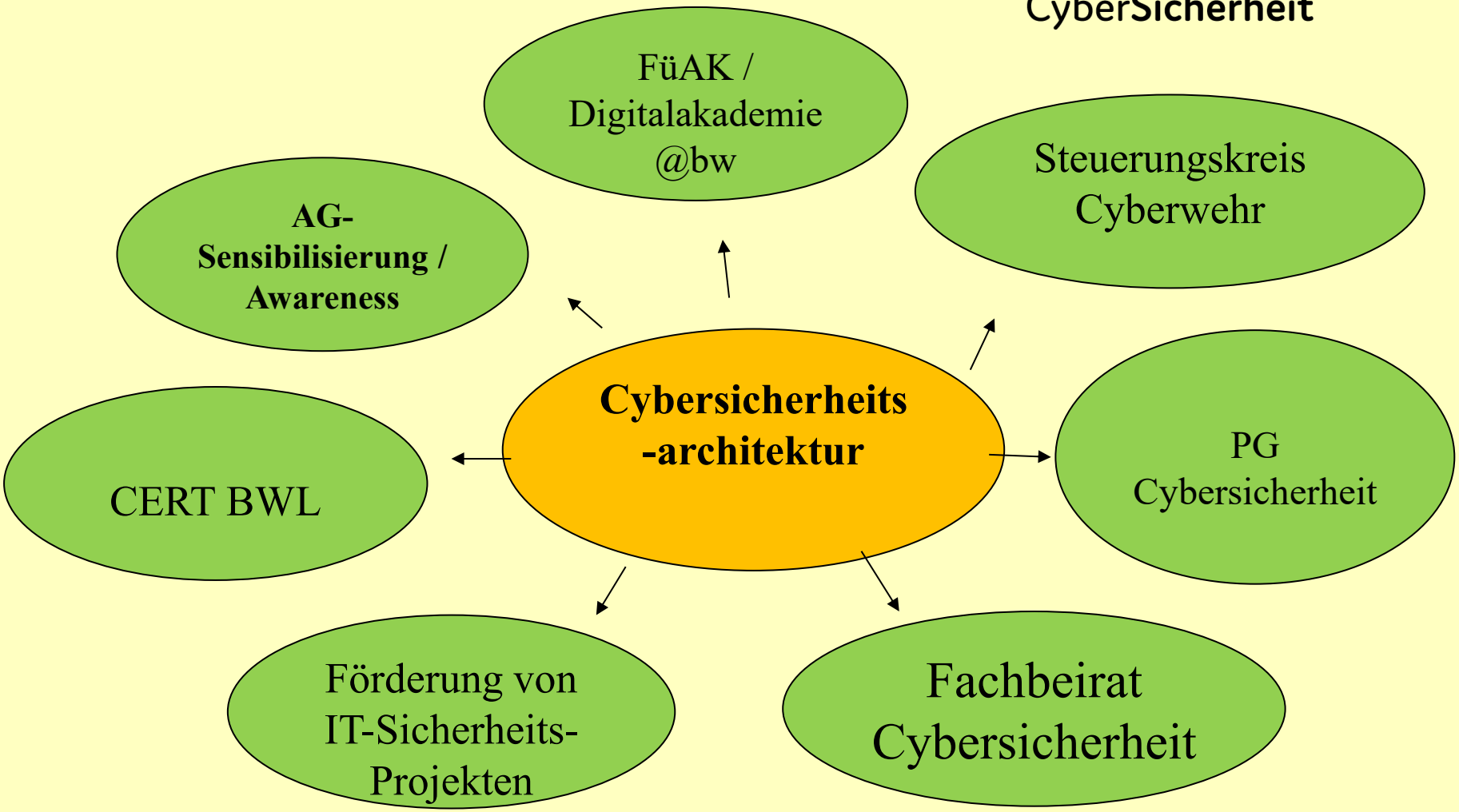
- persönliche Daten, wirtschaftliche Daten und Forschungs-Daten werden immer wertvoller und damit schützenswerter (Treiber KI)
- Damit werden sie immer interessanter für den einzelne Straftäter, für organisierte Kriminalität, für staatliche Interessen, für Konkurenzunternehmen etc.
- Ohne Sicherheit in der Digitalisierung werden wir die Chancen für die Zukunft verspielen. Insbesondere unsere „Kronjuwelen“ müssen geschützt werden.
- Cybersicherheit ist Standortfaktor und Daseinsvorsorge. Eine gute Cybersicherheit schützt unsere persönlichen Daten, unser Wirtschafts-Know How und unsere Forschungs- und Entwicklungsergebnisse. Davon hängt ab, ob wir unseren Wohlstand erhalten können.

digital@bw
CyberSicherheit



Baden-Württemberg
MINISTERIUM FÜR INNERES, DIGITALISIERUNG UND MIGRATION

digital@bw
CyberSicherheit



digital@bw CyberSicherheit

Konsequenzen

- Bessere Zusammenarbeit, Wissens- und Know-Austausch aller Akteure ist die Grundlage einer professionellen Cybersicherheit. Jeder in seinem Silo ist die Welt von Gestern.

- Die Gewährleistung von Informations- und IT-Sicherheit, Datenschutz und Cybersicherheit ist Führungsaufgabe und eine Aufgabe für Vorstände und Geschäftsführungen.

Fragen - die man beantworten sollte

- Was muss ich mir anschauen, um Cybersicherheit zu verbessern ?
- Was kann ich technisch, programmatisch, organisatorisch und personell tun ?
- Welche Standards und Vorlagen kann ich nutzen ?
- Wie könnte ein einfaches Notfallmanagement aussehen ?

Aufbau eines Interims Notfallmanagement

1. Kritische Geschäftsprozesse identifizieren.
2. Risikoanalyse durchführen (Schaden/Wahrscheinlichkeit).
3. Risikoumgang und korrespondierende Maßnahmen festlegen.
4. Strategische Partner suchen und Kontakt aufnehmen.

Cybersicherheit - Handlungsempfehlungen

Ziel 1 Pragmatischer Lösungsansatz

Ziel 2 Unverzügliche Optimierung

Technische Maßnahmen

1. Regelmäßig automatisierte Backups durchführen, diese in gesicherter Form speichern und auf Funktionsfähigkeit testen.

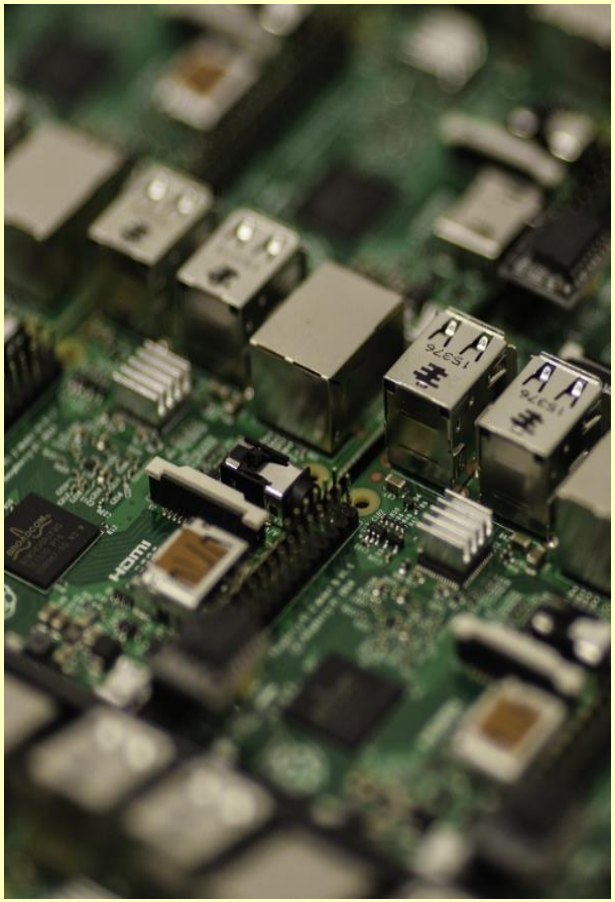
2. Netzwerke und IT-Komponenten sinnvoll voneinander trennen.

3. Zugriffsberechtigungen nur nach Bedarf vergeben und regelmäßig überprüfen.

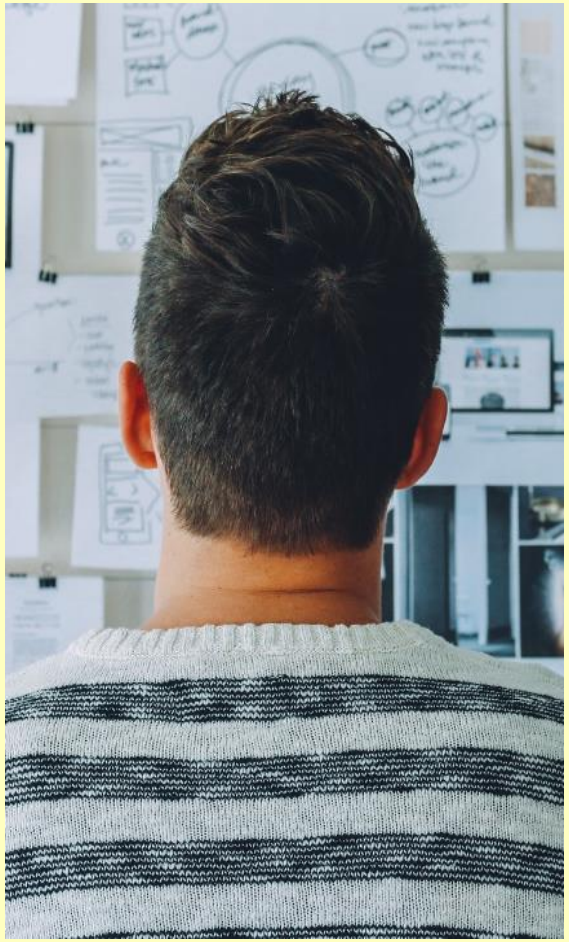
4. Nicht mehr genutzte Hard- und Software entfernen.

5. Beauftragung von Penetrationtests (Netze / Anwendungen).

6. Schatten-IT beseitigen und Alternativen anbieten.



Programmatische Maßnahmen



1. Frühzeitige Überprüfung aktueller und künftiger IT- und Digitalisierungsprojekte auf Cybersicherheits-Aspekte.

2. Kategorisierung der Systeme/Daten nach Kritikalität und regelmäßige Überprüfung der Kategorisierung auf Aktualität.

3. Durchführung einer Daten- und Informationsinventur, inkl. anschließender Auswahl besonders schützenswerter Elemente (Kronjuwelen).

4. Entwicklung einer Organisationskultur, die Informationstechnik als wertschöpfenden Faktor und nicht als Support-Prozess oder gar Hemmnis betrachtet.

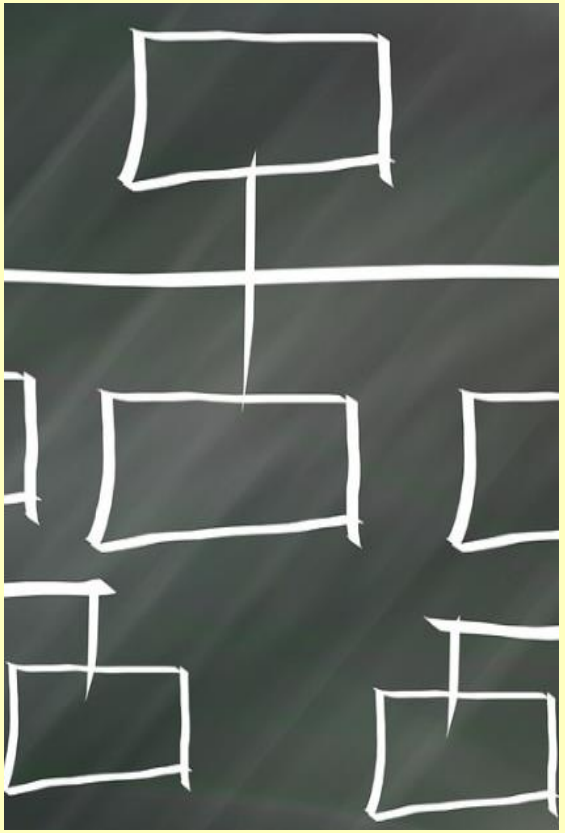
5. Aufbau von Cybersicherheits-Netzwerken mit potentiellen Kooperationskommunen.

Organisatorische Maßnahmen

1. Angemessene organisatorische Verortung des Themas Cybersicherheit im Aufbau der Kommune.

2. Entwicklung und Implementierung von Meldewegen für verdächtige Wahrnehmungen (intern und extern).

3. Schnittstellen zu Prozessen möglicher Partner identifizieren und Anschlussprozesse abstimmen (bspw. IT-Sicherheitsunternehmen, IT-Dienstleister, ITEOS, Zentrale Ansprechstelle Cybercrime der Polizei, CERT-BWL)



Personelle Maßnahmen

1. Durchführung von Sensibilisierungsmaßnahmen anlassbezogen sowie regelmäßig für alle Beschäftigten.

2. Berücksichtigung von IT-Kompetenzen bei der Personalauswahl.

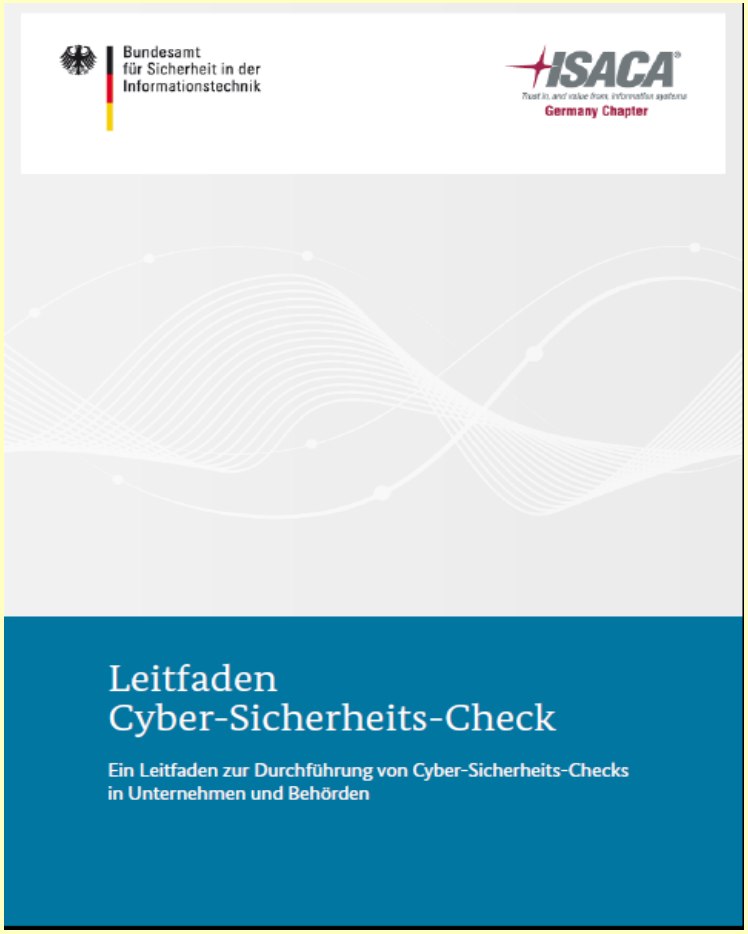
3. Verständnis für Cybersecurity-Maßnahmen auf allen Hierarchieebenen schaffen.

4. Führungskräfte in ihrer Vorbildfunktion bekräftigen.

5. Positives Verhalten bestärken, Unsicherheitskultur sanktionieren.

Beispiele für Info-Material zum Nachlesen

digital@bw CyberSicherheit



Baden-Württemberg
MINISTERIUM FÜR INNERES, DIGITALISIERUNG UND MIGRATION