Abfallwirtschaftsbetrieb Landkreis Ahrweiler **Beschlussvorlage**

Werkleiter: Herr Hurtenbach
Sachbearbeiter: Herr Hurtenbach (Tel. 02641/975-231)
Aktenzeichen:
Vorlage-Nr.: AWB/453/2023

Tagesordnungspunkt

Beratungsfolge:	***Sitzung am:***	***ö/nö:***	***Zuständigkeit:***
Werksausschuss des Abfallwirtschaftsbetriebes	26.04.2023	öffentlich	Kenntnisnahme

Cybersicherheitskonzept für den AWB Ahrweiler

Beschlussvorschlag:

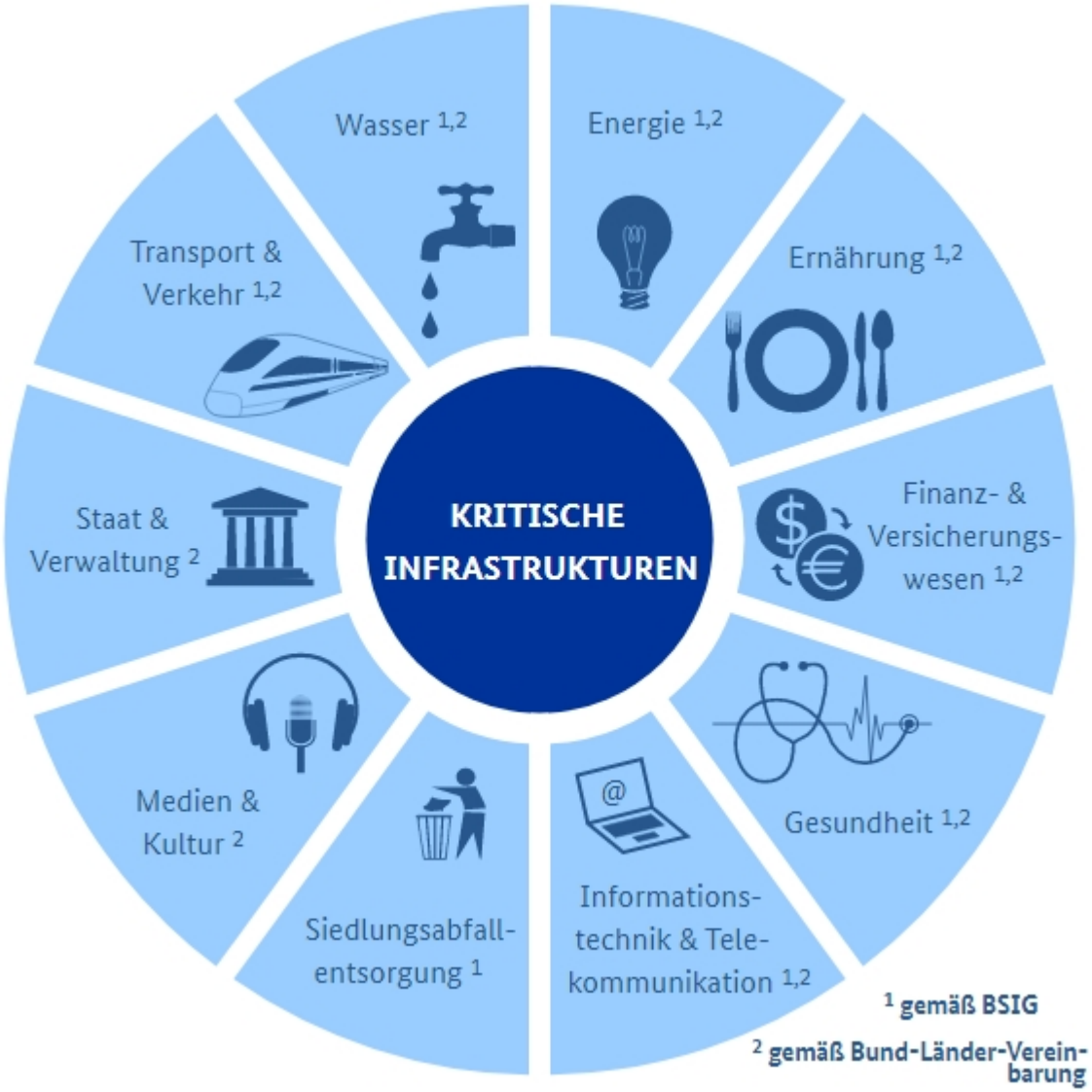
Der Werksausschuss nimmt das Konzept zur Kenntnis.

Nachrichtlich: Nettokosten für den Landkreis Ahrweiler:

Darlegung des Sachverhalts / Begründung:

Nach der Definition des Bundesamtes für Katastrophenschutz Kritische Infrastrukturen (KRITIS): „Organisationen oder 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.“ Kritische Infrastrukturen - BBK (bund.de).

Zu den betroffenen Bereichen gehören:



Die Abfallwirtschaft ist hier in gleich 3 Bereichen betroffen: Siedlungsabfallentsorgung, Staat & Verwaltung sowie Informationstechnik & Telekommunikation.

Im letzten Jahr wurden mehrfach von kriminellen Kräften diese Teile durch Hacking angegriffen. Einige Beispiele sind:

- 2022: Cyberattacke auf die Kreisverwaltung des Rhein-Pfalz-Kreises
- 2022: Cyberattacke auf Donau-Stadtwerke Dillingen-Lauingen

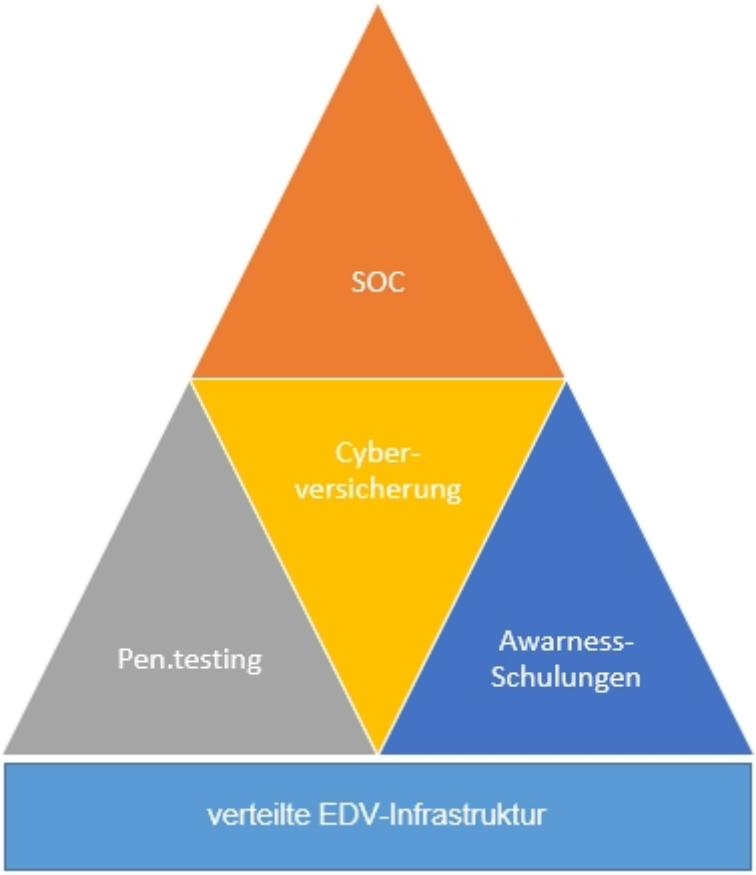
- 2022: Ransomwareattacke auf den Entsorger Otto Dörner

Der AWB nimmt die durch den Ukrainekonflikt gestiegene Bedrohungslage zum Anlass die Cybersicherheit seiner Systeme noch gezielter zu hinterfragen, sie zu härten und möglichst umfangreiche, wirksame präventive Abwehrstrategien zu etablieren.

Wir schätzen das Ausfallrisiko mit Blick auf KRITIS im Falle einer Cyberattacke als differenziert ein. Die Aufgaben des AWB sind unterschiedlich strukturiert. Wir unterscheiden hierbei in die Prozessbereiche:

- der Abholung der Abfälle
- des Umschlags der Abfälle
- der Entsorgung der Abfälle
- der Verwaltung von
    - allg. Administration
    - Gebührendaten
    - Leerungsdaten
    - Leistungsdaten.

Hiervon ausgehend erachten wir im Bereich der Verwaltung unserer Daten hohe Risikolagen. Derzeit verfolgen wir daher eine mehrteilige Strategie auf der Basis einer räumlich und organisatorisch verteilten Infrastruktur:



1) Externe Überprüfung der Vulnerabilität
   Bisher wurde bereits erfolgreich ein sog. Penetrationstest auf die OWASP Top

10 Ziele durchgeführt. Penetrationstest, kurz Pentest(ing), ist der fachsprachliche Ausdruck für einen umfassenden Sicherheitstest einzelner Rechner oder Netzwerke jeglicher Größe. Ein Penetrationstest prüft die Sicherheit von Systembestandteilen und Anwendungen eines Netzwerks oder Softwaresystems mit Mitteln und Methoden, die tauglich sind, um unautorisiert in das System einzudringen (Penetration). Derlei Tests sollen jährlich wiederholt werden.

2) Interne Maßnahmen und Schulungen
   Wir wollen nun einen Maßnahmenplan Ransomware erarbeiten und erstellen einen Katastrophenplan für den Fall eines Angriffs. Daneben haben wir mit den Mitarbeitenden des AWB bereits eine Schulung durchgeführt, um das Sicherheitsbewußtsein zu steigern und dies extern durch gefälschte Hacking-E-Mails überprüfen lassen. Dies soll nun jährlich stattfinden.

3) Rechtzeitige Angriffsfeststellung:
   Der AWB plant aktuell als weitere Sofortmaßnahme in seiner Client-Server-Landschaft ein sogenanntes SIEM (Security Information and Event Management (SIEM) kombiniert die zwei Konzepte Security Information Management (SIM) und Security Event Management (SEM) für die Echtzeitanalyse von Sicherheitsalarmen aus den Quellen Anwendungen und Netzwerkkomponenten. SIEM dient damit der Computersicherheit einer Organisation und ist ein Softwareprodukt, das zentral installiert oder als Cloudservice genutzt werden kann.) einzurichten und durch ein externes SOC (Security Operation Center) Angriffshinweise zu analysieren und durch rechtzeitige Maßnahmen das erfolgreiche Hacking zu verhindern oder wirksam einzudämmen (vgl. TOP 5).

4) Cyberversicherung
   Durch Abdeckung der finanziellen Risiken für Widerherstellung der IT-Landschaft oder die Kosten im Falle des Datendiebstahls finanziellen Schaden für den AWB zu minimieren.

Durch Zusammenarbeit mit Akteuren aus dem Umfeld des Verbandes Kommunaler Unternehmen haben wir an mehrfachen Webinaren und Fortbildungen teilgenommen und so die Notwendigkeit der systematischen Aufarbeitung und Analyse des EDV-Organismus des AWB erkannt. Zusätzlich zu unserem Konzept hinterfragen wir dieses zusätzlich und haben eine externe Fachberatung aus Baden-Württemberg für eine weitergehende gutachterliche Betrachtung angefragt.

Wir bitten um Kenntnisnahme.

Sascha Hurtenbach
Werkleiter