Region der Zukunft
Landkreis Darmstadt-Dieburg

Fraktionsvorlage

Vorlage-Nr.: **1976-2022/DaDi**
Aktenzeichen:

Fachbereich: Fraktion der Freie Wähler/UWG
Rupp, Jörg
Beteiligungen:

Produkt: **1.01.01.02 Gremienmanagement**

Beschlusslauf:

Nr.	*Gremium*	*Status*	*Zuständigkeit*
1.	Kreistag	Ö	Zur Kenntnisnahme

Betreff: **Cybersicherheit (Cybersecurity) in der Kreisverwaltung – Anfrage FW/UWG**

Anfrage der Fraktion von FW/UWG:

In den vergangenen Wochen gab es wieder eine ganze Serie von Cyberangriffen, z.B. Gemeindeverwaltung Egelsbach, Entega Darmstadt, IHK und TH Aschaffenburg, FES Frankfurt usw., sowie auf deutsche Behörden und Ministerien. Noch gut in Erinnerung ist auch der Cyberangriff auf die Kreisverwaltung Anhalt-Bitterfeld, durch den der Katastrophenfall ausgerufen werden musste. Erst nachdem die IT-Strukturen wieder neu aufgebaut waren, konnte nach rd. sechs Monaten der Katastrophenfall wieder aufgehoben werden. Noch heute hat man mit den Folgen des Cyberangriffs zu tun.

Welche fatalen Auswirkungen ein solcher Cyberangriff haben kann, zeigt sich nicht nur in einer fehlenden Erreichbarkeit, sondern auch im schlimmsten Fall bei Dienstleistungen, wie z.B. Überweisungen diverser Sozialleistungen, der Arbeit von Rettungsdiensten, Feuerwehr und im Schulwesen. Im Falle eines Cyberangriffs muss nicht nur die weitere Tätigkeit der Kreisverwaltung, sondern auch der Schutz persönlicher Daten der Einwohner gewährleistet sein.

Deshalb stellt die Fraktion FW/ UWG folgende Fragen:

1. Wer ist für die Cybersicherheit der Kreisverwaltung zuständig und verantwortlich?

   Cybersicherheit ist ein Teil des Themenfeldes der Informationssicherheit. Damit beschreibt man nach Wikipedia (https://de.wikipedia.org/wiki/Informationssicherheit, abgerufen am 5.10.2022) Eigenschaften von technischen oder nicht-technischen Systemen zur Informationsverarbeitung, -speicherung und -lagerung, die die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität sicherstellen. Informationssicherheit dient dem Schutz vor Gefahren bzw. Bedrohungen, der Vermeidung von wirtschaftlichen Schäden und der Minimierung von Risiken.

   Die Zuständigkeit hierfür ist Teil der Organisationsverantwortung der Behördenleitung und im Rahmen der Ausgestaltung u. a. der IT-Leitung.

   Verantwortlich sind, angefangen von den politischen Gremien (u. a. Bereitstellung der für eine gute Cybersicherheit erforderlichen personellen und finanziellen Ressourcen) bis zu

jeder und jedem einzelnen Bediensteten (Kenntnis über sie treffende Gefahren und Berücksichtigung beim eigenen Handeln), alle Teile der Kreisverwaltung.

2. Über wieviele Mitarbeiter*innen verfügt die Kreisverwaltung mit Kenntnissen zur Cybersicherheit und mit welchen Qualifikationen?

   Die Frage lässt sich in der Pauschalität nicht mit einer Zahl oder der Aufzählung erworbener Abschlüsse beantworten.

   Cybersicherheit ist Teil eines Gesamtprozesses im Rahmen eines Informationssicherheitsmanagementsystems (ISMS). Die Rolle einer oder eines Informationssicherheitsbeauftragten ist nicht eingerichtet und besetzt.

   Für alle Bediensteten wurden und werden bereits regelmäßige Schulungs-/Sensibilisierungsmaßnahmen angeboten. Eine jährliche Teilnahme, die Bereitstellung der Haushaltsmittel für das Angebot vorausgesetzt, ist künftig verpflichtend.

3. Ist die Kreisverwaltung nach Einschätzung des Kreisausschusses ausreichend auf einen evtl. Cyberangriff vorbereitet und wie sieht diese Vorbereitung im Detail aus?

   Die Kreisverwaltung stellt täglich Cyberangriffe fest, die soweit dies feststellbar ist ohne Erfolg blieben. Dennoch ist die Antwort: nein.

   Details über Maßnahmenpläne, interne Netzstrukturen und technischen Schutzmaßnahmen zu veröffentlichen, verbietet sich. Der Kreisausschuss bestätigt eine Etablierung der dem Stand der Technik angemessenen technischen und organisatorischen Maßnahmen. Diese orientieren sich an den Vorgaben des IT-Grundschutz nach BSI. Dennoch verbleibt ein nicht unerhebliches Restrisiko bei der Betrachtung des Faktor Mensch.

   Weiterhin empfiehlt der Kreisausschuss dringend, in die weitere Standardisierung des Prozesses sowie entsprechende Tools zu investieren und die systematische Gewährleistung aller kritischer Geschäftsprozesse in Angriff zu nehmen.

4. Welche Redundanzen sind im Falle eines Cyberangriffs eingerichtet bzw. stehen zur Verfügung?

   Die Antwort ist abhängig von der Art und dem Ausmaß des Angriffs. Grundsätzlich ist die IT-Infrastruktur der Kreisverwaltung fehlerredundant nach dem Stand der Technik ausgelegt.

5. Inwiefern besteht eine Zusammenarbeit mit den Kommunen im Landkreis Darmstadt-Dieburg zum Thema Cybersecurity (Cybersicherheit)?

   Es gibt hierzu keine vom Landkreis initiierte Zusammenarbeit, zumal sich die Strukturen und Bedarfe der Kommunen stark von der Kreisverwaltung unterscheiden und für die erforderliche Koordinierung keine personelle Ressource zur Verfügung steht. Der Kreisausschuss sieht es als zielführend an, hier auf der Ebene von Hessen3C, dem Cyber-Competence-Center, zu kooperieren. Selbstverständlich unterstützt der Kreisausschuss Vorhaben von Hessen3C, zuletzt durch die Organisation einer Schulungsreihe für Landkreise und Kommunen im Sommer 2022.

6. Hat die Kreisverwaltung mit angeschlossenen Eigenbetrieben auch schon einen solchen Cyberangriff erlebt und ggf. erfolgreich abgewehrt? Wenn ja, welche?

   Die Frage ist unpräzise. Einen Cyberangriff „erlebt“ zu haben unterstellt, dass dieser

erfolgreich war und dessen Auswirkungen spürbar wurden. Hierauf ist die Antwort: nein. Die Kreisverwaltung ist jedoch dauerhaft und täglich Ziel von Angriffs- und Zugriffsversuchen. Die Reaktion hierauf gehört zum Tagesgeschäft und erfordert ein ständiges Nachhalten.