Beantwortung der Anfrage

Kreis Bergstraße

Vorlage Nr.: **19-1371/1**
erstellt am: 27.05.2025

Abteilung: Moderne Verwaltung, E-Government und IT
Verfasser/in: Dr. Johannes Bunsch
Aktenzeichen: IT

Beantwortung der Anfrage der SPD-Fraktion vom 22.05.2025 zur IT-Sicherheit in der Kreisverwaltung und den Eigenbetrieben im Kreis

Beratungsfolge:

Gremium	Sitzungsdatum	Status	Zuständigkeit
Kreistag		Ö	Kenntnisnahme

Die Anfrage wird wie folgt beantwortet:

Welche Schutzmaßnahmen hat der Kreis für seine IT-Sicherheit ergriffen?

Der Kreis Bergstraße setzt zum Schutz seiner IT-Infrastruktur auf eine Vielzahl von Instrumenten, die technische, organisatorische und regulative Maßnahmen umfassen und die unterschiedlichen Bereiche des IT-Betriebs adressieren (Datenverkehr, Mailverkehr, Netzwerksicherheit, Server, Arbeitsplätze, Softwaresysteme). Dazu zählen insbesondere:

Technische Maßnahmen

- Security Event Management (SIEM)
- Virenscanner
- Firewall
- Sandboxing
- SPAM-Filter
- Network Access Control
- Netzwerk-Scanning
- Analyse laufenden Datenverkehrs
- Ende-zu-Ende Verschlüsselung von Datenverkehr / VPN
- Virtueller Desktop
- Multifaktor-Authentifizierung
- Beseitigung von Schwachstellen in Hardwareanlagen und Softwaresystemen

Für 2025 ist die Einführung eines Security Operation Centers (SOC) sowie eines Mail-Security-Systems geplant.

Organisatorische Maßnahmen

- Backups
- 3 TIER Adminkonzept

- Betrieb kritischer Strukturen im abgesicherten Rechenzentrum der ekom21
- IT-Sicherheitsschulungen, Sensibilisierungsmaßnahmen
- Informationssicherheitskonzeption
- Informationssicherheitsmanagementsystem (ISMS)
- Technische Audits / Pen-Tests
- Zentrales Mobile Device Management
- Passwortmanager

Regulative Maßnahmen

- Dienstanweisungen zu IT, Mobile Arbeitsplätze, elektronische Kommunikation
- Passwortrichtlinie
- Informationssicherheitsrichtlinie

Die Schutzmaßnahmen wurden seit Februar 2022 deutlich ausgeweitet, die obige Aufzählung, die auf die wichtigsten Instrumente fokussiert, spiegelt den aktuellen Stand wider.
Mit Beginn des russischen Angriffskriegs gegen die Ukraine war die Zahl und Schwere der Cyberattacken auf deutsche Behörden sprunghaft angestiegen, auch auf den Kreis Bergstraße. Bereits in den sechs Monaten vor dem Krieg war eine steigende Angriffslage zu erkennen. Mit dem Tag des Kriegsausbruchs stieg diese dann sprunghaft an und hat sich seitdem stetig weiter nach oben entwickelt. Mit allgemeiner Verfügbarkeit von KI-Tools wie ChatGPT hat zudem auch die Qualität der Angriffe deutlich zugenommen. Bislang hat der Kreis Bergstraße dank der ergriffenen Schutzmaßnahmen allen Angriffen standhalten können. Ausfälle beschränkten sich glücklicherweise auf einzelne Arbeitsplätze. Dennoch ist ein erfolgreicher Angriff mehr eine Frage des Wann als des Ob. Letztlich genügt ein Klick z.B. auf eine Phishing-Mail oder der Besuch einer kontaminierten Webseite, um einen Ausfall der gesamten digitalen Betriebsstruktur der Kreisverwaltung herbeizuführen.
Vor diesem Hintergrund hat auch das Thema Resilienz sehr an Bedeutung gewonnen. Ein wichtiger Teil zur Absicherung des Verwaltungsbetriebs ist das sogenannte Business Continuity Management (BCM). Dieses erstellt eine Planung, wie der Betrieb wichtiger Prozesse der Verwaltung aufrecht erhalten werden kann bei einem vollständigen oder Teilausfall der Verwaltungsinfrastruktur (z.B. Ausfall der IT-Systeme, längerfristiger Ausfall eines Gebäudes nach Brand, Wasserschaden etc.). Die Kreisverwaltung hält den Aufbau einer solchen Planung für zwingend erforderlich. Beim erstmaligen Erarbeiten dieser Planungen entsteht ein erheblicher Aufwand. Die hierfür erforderlichen Personal- und Sachressourcen sollen deshalb ab dem Haushalt 2026 beantragt werden.

Werden die Mitarbeiter:innen regelmäßig über neuste Sicherheitsmaßnahmen informiert, weitergebildet und sensibilisiert?

Ja. Es finden Schulungsmaßnahmen über den Kommunalcampus statt. Über aktuelle Bedrohungslagen werden die Beschäftigten über das Intranet unterrichtet. Zudem führt der Kreis kontinuierlich Sensibilisierungsmaßnahmen durch (zurzeit zu Phishing-Attacken).

Wird die Weiterentwicklung der Schutzmaßnahme durch interne oder externe Sicherheitsexperten regelmäßig überprüft und optimiert?

Der Kreis Bergstraße hat einen externen Informationssicherheitsbeauftragten (ISB). Dieser überprüft und kontrolliert die vorhandenen und getroffenen Maßnahmen. Darüber hinaus arbeitet der Kreis am Aufbau der BSI-Basisabsicherung. Dieser Weg wird ebenfalls durch den ISB begleitet. Am Ende des Prozesses erfolgt ein Audit durch das BSI.

Werden aktuelle Bedrohungslagen laufend beobachtet und bewertet?

Ja. Dies geschieht 24/7 sowohl durch technische Systeme als auch unter Einsatz von Personalressourcen (eigene Mitarbeiter sowie Dienstleister).

Gibt es zu aktuellen Sicherheitsereignissen einen Austausch mit Dritten?

Ja. Allgemein müssen Sicherheitsereignisse an den ISB gemeldet werden. Soweit ein Schadensereignis eingetreten ist, muss dieses auch an die Landesbehörden (Hessen3C) gemeldet werden. Die Landesbehörde entscheidet dann, ob sie bei einem laufenden Schadenereignis die Fallbearbeitung übernimmt.
Auch eine Meldung an das Landeskriminalamt, Abteilung Cybercrime, wird bei Schadensereignissen empfohlen. Soweit mit einem erfolgreichen Angriff Datenschutzverletzungen verbunden sind, ist auch eine Meldung an die Landesdatenschutzbeauftragte verpflichtend.

Weiterhin gibt es einen Austausch sowohl im Rahmen des IKZ „ISB“ (Teilnehmer sind hier neben dem Kreis Bergstraße sechs weitere hessische Landkreise) sowie im Rahmen einer entsprechenden Arbeitsgruppe des HLT.

Darüber hinaus gibt es einschlägige Fachveranstaltungen sowie regelmäßige Workshops auf Landes- und Bundesebene organisiert durch Digitalministerien, Verbände (HLT, DLT, Städte- und Gemeindetag) und IT-Sicherheitsbehörden, an denen auch der Kreis Bergstraße aktiv partizipiert.