An die Bürgermeisterin
Frau Claudia Lindlahr
Rathaus
Geistmarkt 1
46446 Emmerich am Rhein

AfD Stadtratsfraktion
Emmerich am Rhein
Geistmarkt 1
46446 Emmerich am Rhein
Mobil: 01556 3390033

Emmerich am Rhein, 13.09.2026

Antrag zur Darstellung Thema IT/Cybersicherheit der Stadt Emmerich – Maßnahmen nach dem Hacking-Angriff auf das Berliner Landesnetz

Sehr geehrte Frau Bürgermeisterin,

die jüngst erfolgte Cyberattacke auf das Berliner Landesnetz mit schwerwiegenden Folgen für die öffentliche Verwaltung kommt eine Signalwirkung zu, die auch unsere Stadt Emmerich in die Pflicht nimmt. Angesichts der wachsenden Bedrohungslage durch staatlich gesteuerte Hackergruppen, Ransomware-Angriffe, Klimaterroristen und gezielte Spionage gegen kommunale Einrichtungen sehen wir uns als AfD-Fraktion im Stadtrat verpflichtet, die Resilienz unserer Stadtverwaltung gegenüber solchen Vorfällen kritisch zu hinterfragen.
Wir erwarten Transparenz über den Stand der IT/Cybersicherheit und den Datenschutz in Emmerich und möglicher abgeleiteter Aktivitäten aus den aktuellen sicherheitsrelevanten Vorfällen in Deutschland.
Vor diesem Hintergrund bitten wir Sie über folgenden Beschlussvorschlag in der nächsten Ratssitzung abstimmen zu lassen:
Der Rat der Stadt Emmerich am Rhein beschließt, die Verwaltung zu beauftragen, zur nächsten Ratssitzung (aktuell 03.11.2026) über das Thema IT/Cybersicherheit der Stadt Emmerich am Rhein unter Berücksichtigung des nachfolgenden Fragenkatalogs zu berichten.

1. Aktueller Stand der IT-Sicherheit und Risikoanalyse

- Welche konkreten Maßnahmen werden nach dem Berliner Vorfall ergriffen, um die IT-Infrastruktur der Stadt Emmerich zu härten (z. B. Validierung und Überprüfung Patch-Management, Netzwerksegmentierung, Deaktivierung veralteter Systeme, CIS Härtungsmaßnahmen)?
- Gibt es einen aktuellen, vollständigen Überblick über alle IT-Systeme der Verwaltung, insbesondere kritische Infrastrukturen (z.B. Bürgerdienste, Finanzwesen, Verkehrstechnik, Energietechnik, Wasserversorgung, Internetknotenpunkte)?
- Wie wird sichergestellt, dass alle Systeme regelmäßig auf Schwachstellen

überprüft werden (automatisierte Scans, manuelle Penetrationstests, Zero-Day-Analysen)?
- Wird eine kontinuierliche Risikoanalyse durchgeführt, und wenn ja, nach welchen Kriterien (z. B. BSI-Standard 200-3)?

2. Zertifizierungen, Compliance und rechtliche Vorgaben

- Ist die IT der Stadt Emmerich oder deren kommunale Rechenzentren nach internationalen Sicherheitsstandards zertifiziert (z. B. ISO/IEC 27001, ISO 27701 für Datenschutz, BSI-Grundschutz)?
    - Falls ja: Wann wurden die letzten Zertifizierungen durchgeführt, und durch wen? Wie hoch ist der Gültigkeitszeitraum?
    - Falls nein: Welche konkreten Schritte sind geplant, um eine Zertifizierung zu erlangen, und bis wann soll dies erfolgen?
- Wie wird die Einhaltung der Datenschutz-Grundverordnung (DSGVO) sowie des Landesdatenschutzgesetzes NRW sichergestellt?
    - Gibt es eine Datenschutz-Folgenabschätzung (DSFA) für alle kritischen IT-Systeme, und wenn ja, wann wurde diese zuletzt aktualisiert?
    - Werden Datenminimierung und Zweckbindung bei der Verarbeitung personenbezogener Daten in der Verwaltung konsequent umgesetzt?
- Welche rechtlichen Vorgaben (z. B. KRITIS-Verordnung, NIS2-Richtlinie) sind für die Stadt Emmerich relevant, und wie wird deren Umsetzung überwacht?

3. Schulungen, Sensibilisierung und Personalressourcen

- Wie viele Mitarbeiter der Stadtverwaltung wurden in den letzten zwei Jahren zu Themen wie Cybersecurity, Phishing, Social Engineering oder Datenschutz geschult?
    - Gibt es ein verpflichtendes Schulungsprogramm für neue Mitarbeiter, und wie oft wird dieses wiederholt?
- Wurden in den letzten zwei Jahren simulierte Phishing-Angriffe durchgeführt, und wenn ja:
    - Wie hoch war die Klickrate der Mitarbeiter?
    - Welche Konsequenzen wurden bei erfolgreichen Angriffen gezogen (z. B. Nachschulungen)?
- Wie wird die Sensibilisierung der Führungsebene für Cyberrisiken sichergestellt?
- Gibt es einen Mangel an qualifiziertem Personal im Bereich IT-Sicherheit, und wenn ja, wie wird diesem begegnet?

4. Audits, Überprüfungen und Third-Party-Risiken

- Wann wurde zuletzt ein externes IT-Sicherheitsaudit durchgeführt, und welche kritischen Mängel wurden dabei festgestellt?
    - Wird ein regelmäßiger Turnus für Audits eingehalten (z. B. jährlich oder alle zwei Jahre)?
    - Wie schnell werden Empfehlungen aus Audits umgesetzt, und gibt es eine Dokumentation der Fortschritte?
- Wie wird die Sicherheit von Drittanbieter-Systemen überwacht (z. B. Cloud-Dienste, externe IT-Dienstleister, Software-as-a-Service)?
    - Gibt es vertragliche Sicherheitsklauseln mit allen externen Partnern?
    - Werden Lieferkettenrisiken (z. B. durch Abhängigkeiten von ausländischen IT-Herstellern) berücksichtigt?

5. Notfallpläne, Incident Response und Wiederherstellung

- Gibt es einen aktuellen, schriftlich dokumentierten Notfallplan (Incident Response Plan) für Cyberangriffe?
  - Wann wurde dieser Plan zuletzt überprüft und aktualisiert?
  - Wer ist für die Umsetzung im Ernstfall verantwortlich, und wie ist die Alarmierungskette geregelt?
- Wie wird sichergestellt, dass im Falle eines Angriffs die Daten schnellstmöglich wiederhergestellt werden können?
  - Gibt es ein mehrstufiges Backup-Konzept (lokal, extern, offline)?
  - Wie oft werden Backup- und Restore-Tests durchgeführt, und wie lange dauert die Wiederherstellung im Ernstfall?
- Gibt es eine klare Kommunikationsstrategie für den Fall eines erfolgreichen Angriffs?
  - Wie wird die Transparenz gegenüber Bürgern, Medien und Aufsichtsbehörden sichergestellt?
  - Wird ein Krisenstab für IT-Sicherheitsvorfälle eingerichtet, und wer gehört diesem an?

6. Verantwortlichkeiten, Zusammenarbeit und Berichterstattung

- Wer ist in der Stadtverwaltung verantwortlich für die IT-Sicherheit, und welche Qualifikation hat diese Person?
  - Gibt es eine eigene IT-Sicherheitsabteilung, oder wird diese Aufgabe extern vergeben?
- Wie ist die Zusammenarbeit mit externen Stellen geregelt (z. B. BSI, CERT-Bund, Landes-CERT NRW, Polizei)?
  - Werden Lageberichte oder Warnmeldungen dieser Stellen zeitnah an die Verwaltung weitergeleitet und umgesetzt?
- Wie wird die Kommunikation mit dem Stadtrat über IT-Sicherheitsthemen sichergestellt?
  - Gibt es regelmäßige Berichte an den Rat oder die Öffentlichkeit?
  - Werden Sicherheitsvorfälle oder Datenschutzverletzungen transparent dokumentiert und gemeldet?

7. Finanzielle und technische Ausstattung

- Wie hoch ist das jährliche Budget für IT-Sicherheit in der Stadtverwaltung?
  - Wird dieses Budget ausreichend bemessen, um moderne Sicherheitslösungen (z. B. Next-Generation Firewalls, EDR-Systeme, SIEM-Lösungen) zu finanzieren?
- Gibt es ausreichend Mittel für Investitionen in neue Technologien (z. B. KI-gestützte Bedrohungserkennung, Zero-Trust-Architekturen)?
- Werden ausreichend Ressourcen für die Wartung, Überwachung und Aktualisierung der IT-Systeme bereitgestellt?

8. Transparenz und Bürgerinformation

- Gibt es eine öffentliche Dokumentation der IT-Sicherheitsmaßnahmen der Stadt Emmerich (z. B. auf der städtischen Website)?
- Wie wird sichergestellt, dass Bürger im Falle eines Datenschutzvorfalls transparent informiert werden?
- Wurden in den letzten fünf Jahren Sicherheitsvorfälle oder Datenschutzverletzungen gemeldet, und wenn ja:
    - Wie wurden diese behandelt?
    - Welche Lehren wurden daraus gezogen?

9. Technische Gegenmaßnahmen & Infrastruktur

- Moderne Sicherheitsarchitekturen:
    - Wird eine Zero-Trust-Architektur oder Microsegmentierung des Netzwerks umgesetzt?
    - Gibt es Multi-Faktor-Authentifizierung (MFA) für alle kritischen Systeme (z. B. Bürgerportale, Finanzsysteme)?
    - Wie wird die Verschlüsselung von Daten sichergestellt (z. B. Ende-zu-Ende-Verschlüsselung, Verschlüsselung von Backups)?
- Überwachung & Erkennung:
    - Wird ein SIEM-System (Security Information and Event Management) eingesetzt, um Angriffe in Echtzeit zu erkennen?
    - Gibt es Intrusion Detection/Prevention Systems (IDS/IPS) in der Netzwerkinfrastruktur?
    - Wie wird die Anomalieerkennung (z. B. durch KI oder maschinelles Lernen) genutzt?
- Sicherheit von Endgeräten:
    - Werden Endpoint Detection and Response (EDR)-Lösungen eingesetzt?
    - Wie wird die Sicherheit von mobilen Geräten (z. B. Diensthandys, Tablets) sichergestellt?
    - Wie wird die Sicherheit von Workstationgeräten sichergestellt; insbesondere im Homeoffice (z.B. VPN, Notebooks, SINA-Clients).

Sollten einzelne Punkte nicht vollständig beantwortet werden können, bitten wir um eine detaillierte Begründung sowie um Angaben zu den geplanten Lösungswegen und/oder alternativen Terminen zur Beantwortung.

Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Mit freundlichen Grüßen,

Michael Lümmen