Rhein-Kreis Neuss

Neuss/Grevenbroich, 23.09.2026

ZD2 - IT-Service und Digitalisierung

Tischvorlage

Sitzungsvorlage-Nr. ZD2/1539/XVIII/2026

Gremium	Sitzungstermin	Behandlung
Kreistag	30.09.2026	öffentlich

Tagesordnungspunkt:

Tischvorlage: Anfrage der CDU- und FDP-Kreistagsfraktion zum Thema "IT-Sicherheit und Resilienz der Kreisverwaltung vor dem Hintergrund des Cyberangriffs auf das Berliner Landesnetz" vom 21.09.2026 und Antwort der Verwaltung

Sachverhalt:

Die Verwaltung nimmt wie folgt Stellung:

1. Welche Erkenntnisse zieht die Kreisverwaltung gemeinsam mit der ITK Rheinland aus dem jüngsten Cyberangriff auf das Berliner Landesnetz und wird derzeit geprüft, ob sich hieraus zusätzlicher Handlungsbedarf für die IT-Sicherheitsstrukturen des Rhein-Kreises Neuss ergibt?

Das Thema des Cyberangriffs in Berlin wurde im gemeinsamen Arbeitskreis mit den Kommunen und der ITK thematisiert. Die ITK trifft ihrerseits Vorkehrungen, um Cyber-Attacken jeglicher Art abwehren, bzw. Anomalien feststellen zu können.
Die Kommunen müssen eigene Sicherheitsmaßnahmen ergreifen, damit die Infrastruktur vor Ort in erforderlichem Umfang geschützt wird. Die IT-Sicherheits-beauftragten der Kommunen stehen in ständigem Kontakt mit der IT-Sicherheit der ITK.

Der Rhein-Kreis Neuss hat für die eigene Infrastruktur einen Servicevertrag mit einem externen Dienstleister geschlossen, der die Systeme (Client und Server) rund um die Uhr überwacht und auf Anomalien oder Angriffe überprüft. Zudem besteht eine Rufbereitschaft von IT-Mitarbeitern des Rhein-Kreises Neuss, die ebenfalls rund um die Uhr eine Erreichbarkeit sicherstellt, um auf Meldungen sofort und jederzeit reagieren zu können.

Die Sicherheitsmaßnahmen werden ständig auf Erweiterungs- und Verbesserungs-möglichkeiten geprüft. Erkenntnisse und Wissensstände werden zwischen den IT-Sicherheitsbeauftragten und der ITK ausgetauscht.

2. In welcher Form stehen die Kreisverwaltung und die ITK Rheinland mit den zuständigen Stellen auf Landes- und Bundesebene im Austausch über aktuelle

Cyberbedrohungen und Erkenntnisse aus größeren Cyberangriffen auf öffentliche Verwaltungen?

Die ITK und die Kommunen werden zeitnah vom Computer Emergency Response Team (CERT) des Landes über neue Schwachstellen informiert. Die Zusammenarbeit zwischen Bund und Ländern erfolgt über den Verwaltungs-CERT-Verbund (VCV).

3. Da Phishing-Mails häufig ein erstes Einfallstor für Ransomware-Gruppen darstellen: In welchem Umfang werden die Beschäftigten des Kreises im Bereich der IT-Sicherheit geschult und sensibilisiert und werden ergänzend unangekündigte Phishing-Simulationen durchgeführt?

Der Rhein-Kreis Neuss führt seit mehreren Jahren eine kontinuierliche Schulung aller Mitarbeitenden der Kreisverwaltung im Bereich der IT-Sicherheit durch. Ein Themenfeld dieser Schulungen ist das Erkennen von Phishing-Mails und der richtige Umgang mit diesen Mails. Es werden in bestimmten Zyklen eigene Phishing-Simulationen durchgeführt, bei denen den Nutzern durch das System eine Rückmeldung gegeben wird, falls sie eine simulierte Phishing-Mail nicht erkannt haben. Die Statistiken zeigen, dass die Schulungen erfolgreich verlaufen und die Fehlerquote seit der Einführung des Systems erheblich gesunken ist. Die Schulungen und Simulationen werden auch zukünftig fortgeführt.

Anlagen:
20260930 Anfrage IT-Sicherheit und Resilienz der Kreisverwaltung vor dem Hintergrund des Cyberangriffs auf das Berliner Landesnetz