KREISTAGSFRAKTION RHEIN-KREIS NEUSS
SPD

Fraktionsbüro
Platz der Republik 11
41515 Grevenbroich

Tel. +49 2181 2250 20
Fax +49 2181 2250 40
kreistagsfraktion@spd-kreis-neuss.de

BÜNDNIS 90 DIE GRÜNEN
KREISTAGSFRAKTION RKN

Fraktionsbüro
Schulstr.1
41460 Neuss

Tel. +49 2131 1666 81
Fax +49 2131 1666 83
fraktion@gruene-rkn.de

An den Vorsitzenden des Finanzausschusses
Herrn Stefan Schmitz, Kreisverwaltung

23. Februar 2024

Sitzung des Finanzausschusses am 5. März 2024

Antrag: IT-Sicherheit endlich ernst nehmen: Personal aufstocken und Cybersicherheit strategisch weiterentwickeln

Sehr geehrter Herr Schmitz,

die **Kreistagsfraktionen von SPD und BÜNDNIS 90/DIE GRÜNEN** beantragen, folgenden Beschluss zu fassen:

- Der Rhein-Kreis Neuss beschließt, den Bereich der IT-Sicherheit schnellstmöglich um eine Vollzeitstelle zu erweitern. So soll sichergestellt werden, dass die IT-Sicherheit zu jeder Zeit – auch in Abwesenheit wegen Krankheit oder Urlaub – gewährleistet werden kann. Hierzu werden die entsprechenden Mittel im Haushalt bereitgestellt.
  Zudem ist bei der weiteren Ausgestaltung des Bereichs eine Trennung zwischen der operativen Ebene und der IT-Sicherheit aus Gründen der Sicherheit und Effektivität zu erwägen.
  Darüber hinaus ist zu prüfen, ob weitere Personalstellen und finanzielle Mittel zur Erreichung dieses Ziels sowie zur strategischen Weiterentwicklung der Cybersicherheit notwendig sind.

Begründung:

Wenn auf einmal nichts mehr geht: Eine Vielzahl von Kommunen haben zuletzt erfahren müssen, was es bedeutet, wenn ihre Infrastruktur von Hackern angegriffen wird. Nach dem Hackerangriff auf den IT-Dienstleister „Südwestfalen-IT“ in der Nacht zum 30. Oktober 2023 war in 70 Kommunen in Nordrhein-Westfalen teils für mehrere Wochen an die Abwicklung von Behördengängen nicht zu denken. So standen in einigen Städten und Gemeinden nur noch Block und Stift zur Bearbeitung von Bürger*innenanliegen zur Verfügung. Aber auch automatisierte Rechnungen konnten nicht mehr bezahlt werden, Lastschriftmandate nicht eingelöst oder Straßenbauprojekte nicht mehr vergeben werden. Es herrschte Chaos in den betroffenen Kommunen. Besonders betroffen war unter anderem die Stadt Olpe, die durch den Hackerangriff auch auf ihren Haushaltsentwurf für 2024 nicht mehr zugreifen konnte.

Nach Veröffentlichung des forensischen Berichts kommen Expert*innen nun zu dem Ergebnis, dass die Angreifer auf die „Südwestfalen-IT“ ein leichtes Spiel hatten, weil keine "Multifaktor-Authentifizierung" verwendet worden ist. Ferner werden Kommunen von Expert*innen als leichtes Angriffsobjekt für Hackerangriffe bewertet.

Aus Sicht der Kreistagsfraktionen von SPD und BÜNDNIS 90/DIE GRÜNEN müssen alle Anstrengungen unternommen werden, um einen erfolgreichen Hackerangriff auf die Strukturen des Rhein-Kreises Neuss zu vermeiden. In der Sitzung des Ausschusses für

KREISTAGSFRAKTION RHEIN-KREIS NEUSS
SPD

Fraktionsbüro
Platz der Republik 11
41515 Grevenbroich

Tel. +49 2181 2250 20
Fax +49 2181 2250 40
kreistagsfraktion@spd-kreis-neuss.de

BÜNDNIS 90 DIE GRÜNEN
KREISTAGSFRAKTION RKN

Fraktionsbüro
Schulstr.1
41460 Neuss

Tel. +49 2131 1666 81
Fax +49 2131 1666 83
fraktion@gruene-rkn.de

Innovation, Digitalisierung und Standortmarketing am 4. Mai 2023 stellte der IT-Sicherheitsbeauftragte der Verwaltung die aktuelle Situation im Rhein-Kreis Neuss – im Zuge der Vorstellung des Jahresberichts zur IT-Sicherheit 2022 - dar.

Die Ausführungen unterstrichen, dass die momentane personelle Situation nicht ausreichend ist, um die Cybersicherheit im Kreis bestmöglich zu gewährleisten. So heißt es in der Sitzungsvorlage-Nr. VI/2608/XVII/2023 „Zum Tagesgeschäft der IT der Kreisverwaltung gehört es deshalb zunehmend, potentielle Schwachstellen für Cyber-Angriffe zu lokalisieren und abzustellen und die Beschäftigten zu schulen und zu sensibilisieren." Auf Nachfrage wurde deutlich, dass es zurzeit keine Vollzeitstelle in der Verwaltung gibt, die sich ausschließlich um die Sicherstellung der IT-Sicherheit kümmert. Vielmehr gibt es eine Überschneidung zwischen dem operativen Geschäft und der IT-Sicherheit. Das erscheint aus Gründen der Sicherheit und Effektivität fraglich. Die formell benannten IT-Sicherheitsbeauftragten (75 Prozent sowie 25 Prozent Stellenanteil) können durch ihre Arbeitsleistung für zusätzliche IT-Aufgabenbereiche und der maßgeblichen Beteiligung am operativen Tagesgeschäft den zugestandenen Zeitanteilen nicht gerecht werden. Es bedarf einer Umverteilung der andersartigen Hauptaufgaben, um der Übertragung der Rolle als IT-Sicherheitsverantwortliche in der Praxis gerecht zu werden.

Ferner ist auch die Verantwortlichkeit für die Cybersicherheit im Falle von Urlaub oder Krankheit bedenklich. Aus den genannten Gründen braucht es umgehend personelle Verstärkung für die IT-Sicherheit.

Damit der Bereich der IT-Sicherheit zudem für die Zukunft aufgestellt werden kann, auch vor dem Hintergrund von immer häufiger werdenden und komplexeren Angriffen, muss eine Weiterentwicklung des Bereichs erfolgen. In den Jahren 2022 und 2023 wurden beim Rhein-Kreis Neuss zusätzliche Sicherheitstechniken zum Einsatz gebracht, um die Cyber-Resilienz maßgeblich zu stärken. Die hinzugewonnen Schutztechnologien brauchen eine laufende Betreuung und unterliegen einem kontinuierlichen Verbesserungsprozess (PDCA-Zyklus). Die Auslastung der zentralen IT-Steuerung ist dadurch zwangsläufig erheblich gestiegen. In diesem Zusammenhang ist zu prüfen, wie das personelle Konzept für die Cybersicherheit strategisch für die Zukunft ausgerichtet werden kann und muss und ggf. durch weiteres Personal aufzustocken ist. Die Anforderungen der Cyberversicherung sind ebenfalls zu berücksichtigen. Hierzu ist dem Ausschuss für Innovation, Digitalisierung und Standortmarketing zu berichten.

Mit freundlichen Grüßen

Udo Bartsch (SPD)	Petra Schenke (GRÜNE)	Dirk Schimanski (GRÜNE)	Christina Borggräfe
Fraktionsvorsitzender	Fraktionsvorsitzende	Fraktionsvorsitzender	stllv. Landrätin (SPD)

(1) https://www.tagesschau.de/inland/regional/nordrheinwestfalen/wdr-hacker-angriff-suedwestfalen-it-raeumt-schwere-sicherheitsluecken-ein-100.html
(2) https://www.zeit.de/2024/05/hackerangriff-kommunen-kreis-olpe-digitalisierung