LANDTAG RHEINLAND-PFALZ
18. Wahlperiode

Drucksache 18/4875
zu Drucksache 18/4722
29. 11. 2022

Antwort

des Ministeriums für Arbeit, Soziales, Transformation und Digitalisierung

auf die Kleine Anfrage des Abgeordneten Patrick Kunz (FREIE WÄHLER)
– Drucksache 18/4722 –

Cyberangriffe gegen die Kreisverwaltung Rhein-Pfalz-Kreis

Die **Kleine Anfrage – Drucksache 18/4722 –** vom 15. November 2022 hat folgenden Wortlaut:

Der Hackerangriff Ende Oktober 2022 auf die Kreisverwaltung des Rhein-Pfalz-Kreis in Ludwigshafen zeigt uns, wie schnell eine Behörde über Monate auf Eis gelegt werden kann. Mit Recht stellen sich nun die Mitarbeiterinnen und Mitarbeiter in meinem Wahlkreis die Frage: „Wie sicher sind unsere Behörden?“ Aus Sicht der FREIEN WÄHLER müssen nun Cyberabwehrmaßnahmen für die Verwaltungen des Landes Rheinland-Pfalz geschaffen werden.
Vor diesem Hintergrund frage ich die Landesregierung:

1. Wie sicher sind die Landesbehörden gegen Cyberangriffe im Wahlkreis 39?
2. Gilt der Cyberschutz aus Frage 1 für alle Landesbehörden?
3. Kann die landeseigene Cyber-Abwehr einen Cyber-Schutzschild aufbauen, in den sich die Kommunal- und Kreisverwaltungen integrieren lassen?
4. Wie viele Hackerangriffe werden pro Monat gegen die Landesbehörden im Wahlkreis 39 verzeichnet?
5. Wie viele Hackerangriffe werden pro Monat gegen die Kommunal- und Kreisverwaltungen im Wahlkreis 39 registriert?

Das **Ministerium für Arbeit, Soziales, Transformation und Digitalisierung** hat die Kleine Anfrage namens der Landesregierung mit angefügtem Schreiben beantwortet.

Druck: Landtag Rheinland-Pfalz, 2. Dezember 2022

E: 29.11.2022
18/4875

RheinlandPfalz
MINISTERIUM FÜR ARBEIT, SOZIALES, TRANSFORMATION UND DIGITALISIERUNG

Ministerium für Arbeit, Soziales, Transformation und Digitalisierung
Postfach 31 80 | 55021 Mainz

Präsident des
Landtags Rheinland-Pfalz
55116 Mainz

DER MINISTER

Bauhofstraße 9
55116 Mainz
Telefon 06131 16-0
Telefax 06131 16-2452
Mail: poststelle@mastd.rlp.de
www.mastd.rlp.de

29. November 2022

nachrichtlich:

Staatskanzlei
55116 Mainz

Kleine Anfrage des Abgeordneten Patrick Kunz (Freie Wähler)
betr. Cyberangriffe gegen die Kreisverwaltung Rhein-Pfalz-Kreis
- Drucksache 18/4722 -

Die Kleine Anfrage beantworte ich namens der Landesregierung wie folgt:

Zu 1. und 2.:

Für die landeseigenen Einrichtungen (darunter auch die 21 im Wahlkreis 39 gelegenen Einrichtungen mit Ausnahme des Studienseminars Speyer) betreibt der Landesbetrieb Daten und Information (LDI) ein konvergentes Netzwerk zur Übertragung von Daten sowie Sprach-und Videoinformationen für die Landesverwaltung, das sogenannte rlp-Netz. Dieses Landesnetz ist nach der IT-Grundschutz-Methodik des Bundesamtes für Informationssicherheit (BSI) zertifiziert und wird regelmäßig von einem externen Auditor re-zertifiziert. Diese Zertifizierung belegt, dass zum einen nach den Anforderungen des Bundesamtes für Informationssicherheit ein angemessenes Schutzniveau für die Datensicherheit gewährleistet ist, zum anderen, dass ein wirksames Informationssicherheitsmanagementsystem (ISMS) implementiert und gelebt wird, um Informationssicherheit zu überwachen, zu steuern und kontinuierlich weiter zu entwickeln.

Lediglich das Studienseminar Speyer verfügt über eine eigene Internetanbindung, die von einem externen Dienstleister bereitgestellt wird und der auch die gesamte IT-Infrastruktur betreibt. Gängige Sicherheitsmechanismen, wie mehrstufige Firewall, E-Mail-Filter oder Virenschutz, sind umgesetzt.

Die Verwaltungsvorschrift Leitlinie zur Informationssicherheit der Landesverwaltung sieht unter anderem vor, dass die Behörden beziehungsweise deren Leitungen durch Informationssicherheitsbeauftragte unterstützt werden. Diese koordinieren die Fragen, Themen und Maßnahmen der Informationssicherheit auf ihrer jeweiligen Ebene und tragen damit zum Schutz vor Cyberangriffen bei.

Informationssicherheit ist eine dauerhafte Aufgabe und muss kontinuierlich weiterentwickelt werden. Eine hundertprozentige Sicherheit kann nicht gewährleistet werden. Die Landesregierung arbeitet daher stetig am weiteren Aufbau und Ausbau ihres Informationssicherheitsmanagements.

Zu 3.:

Bereits nach der Verabschiedung der Leitlinie Informationssicherheit für die Verwaltungen der Länder und des Bundes durch den IT-Planungsrat im Jahr 2013 hat die Landesregierung zur Umsetzung der Leitlinie die Zusammenarbeit mit den Kommunalen Spitzenverbänden gesucht. Im Rahmen eines gemeinsamen Projektes „Informationssicherheit bei den Kommunalverwaltungen in Rheinland-Pfalz“ (mit einer Laufzeit von 2014-2019) wurden für die Kommunen Hilfsmittel zur Einführung des IT-Grundschutzstandards des Bundesamtes für Informationssicherheit (BSI) erarbeitet sowie ein CERT (CERT-kommunal-rlp) beim kommunalen IT-Dienstleister KommWis GmbH aufgebaut.

Die Dienste des CERT der Landesverwaltung (CERT-rlp) wurden dem CERT-kommunal-rlp - hier insbesondere der Warn- und Informationsdienst des Landes - zur Verfügung gestellt. Außerdem erhielten alle Kommunen Zugriff auf die Informationssicherheitsplattform des Landes. Auf dieser gemeinsamen Plattform wurde auch ein Bereich für Informationen des CERT-kommunal-rlp eingerichtet.

Es hat sich über die Jahre eine vertrauensvolle Zusammenarbeit zwischen dem CERT-rlp und dem CERT-kommunal-rlp in Rheinland-Pfalz entwickelt, die kontinuierlich ausgebaut wird.

Auf Basis der gemeinsamen Vereinbarung zwischen dem Land und den kommunalen Spitzenverbänden auf dem Gebiet der Informationssicherheit soll diese Kooperation weiter vertieft werden. Verschiedene Maßnahmen zur Unterstützung der Kommunen sind in der landesinternen Abstimmung.

Seit Beginn des Russland-Ukraine-Krieges besteht insbesondere für Betreiber kritischer Infrastrukturen (KRITIS) eine erhöhte Gefährdung durch gezielte Cyberangriffe. Der rheinland-pfälzische Verfassungsschutz hat deshalb bereits Ende Februar 2022 seine Unterstützungsleistungen im Hinblick auf die Cybersicherheit ausgebaut. So werden regelmäßig aktuelle technische Absicherungsmöglichkeiten für die IT-Infrastruktur von KRITIS-Betreibern, Unternehmen und öffentlicher Verwaltung zur Verfügung gestellt. Auch zahlreiche Kommunal- und Kreisverwaltungen nutzen das Angebot bereits. Am 24. Oktober 2022 wurde zudem das neu eingerichtete Sicherheitsportal Cyberschutz Rheinland-Pfalz (www.cyberschutz.rlp.de) gestartet. Dort werden die angebotenen Absicherungsmöglichkeiten und ihre Verwendung gezeigt. Darüber hinaus wird zu den Gefahren durch Cyberspionage und -Sabotage sensibilisiert und zum Verhalten im Fall eines Cyberangriffs beraten.

Zu 4.:

Für die zurückliegenden 12 Monate liegen der Landesregierung für die an das rlp-Netz angeschlossenen Landeseinrichtungen im Wahlkreis 39 keine Meldungen bezüglich Hackerangriffen vor. Daten, die über diesen Zeitraum hinausgehen, werden nicht vorgehalten.

Zu 5.:

Der Landesregierung liegen hierzu keine Zahlen vor.

Hackerangriffe auf die kommunale Infrastruktur werden durch die Kommunal- und Kreisverwaltungen an das zuständige kommunale CERT-kommunal-rlp gemeldet. Eine Meldepflicht für die Kommunen an das CERT-kommunal-rlp besteht jedoch nicht.

Alexander Schweitzer