LANDTAG RHEINLAND-PFALZ
18. Wahlperiode

Drucksache 18/4890
zu Drucksache 18/4734
01. 12. 2022

Antwort

des Ministeriums für Arbeit, Soziales, Transformation und Digitalisierung

auf die Kleine Anfrage der Abgeordneten Lisa-Marie Jeckel (FREIE WÄHLER)
– Drucksache 18/4734 –

Hackerangriffe und Datensicherheit im Rhein-Pfalz-Kreis

Die **Kleine Anfrage – Drucksache 18/4734 –** vom 15. November 2022 hat folgenden Wortlaut:

Im Oktober wurde die Verwaltung des Rhein-Pfalz-Kreises Opfer eines gezielten Hackerangriffes. Alle 600 Computer der Kreisverwaltung seien von dem Hackerangriff betroffen, berichtete Landrat Clemens Körner (CDU) dem SWR. Ebenso äußerte er sich im selben Bericht, dass es Monate dauern könnte, bis die Kreisverwaltung wieder regulär arbeiten kann. Das schnelle Eingreifen der IT-Experten sei es, nach Körner, zu verdanken gewesen, dass die Geräte und Systeme abgeschaltet wurden, bevor schlimmerer Schaden angerichtet werden konnte. Am Hauptsitz des Rhein-Pfalz-Kreises in Ludwigshafen soll nun nach Angaben einer Sprecherin eine „Notverwaltung“ eingerichtet werden. Die Kreisverwaltung plant, Arbeitsplätze an mehreren PCs einzurichten, die unabhängig vom Computernetz der Behörde laufen sollen. Für Innenminister Michael Ebling (SPD) ist klar, dass Städte und Kreise in Rheinland-Pfalz eine „gute Beratung“ benötigen.
Vor diesem Hintergrund frage ich die Landesregierung:

1. Wie oft wurden in Rheinland-Pfalz bereits „Cyberangriffe“ durch die „Vice-Society“ verübt (bitte aufgeschlüsselt nach Vorfall und Zeitraum)?
2. Welche Präventivmaßnahmen werden derzeit vom Land Rheinland-Pfalz im Bereich der „Cybersicherheit“ Kommunen zum Schutz ihrer IT empfohlen?
3. Welche Beratungen werden derzeit Städten und Kreisen angeboten, um sich vor „Cyberangriffen“ besser zu schützen?
4. Gibt es derzeit vom Land Rheinland-Pfalz Richtlinien oder Leitfäden für Städte und Kommunen, wie diese bei einem erfolgten Angriff reagieren sollten?
5. Wie viele Kommunen besitzen derzeit einen Plan für eine „Notverwaltung“, wie sie derzeit im Rhein-Pfalz-Kreis angewendet wird?
6. Wie viele „Cyberangriffe“ wurden seit dem Jahr 2017 durch Einzelpersonen verübt (bitte aufgeschlüsselt nach Anzahl der Vorfälle und Jahr)?
7. Wie viele „Cyberangriffe“ wurden seit dem Jahr 2017 durch mehrere Personen gemeinsam verübt (bitte aufgeschlüsselt nach Anzahl der Vorfälle und Jahr)?

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: 01.12.2022
18/4890

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

nachrichtlich:

Staatskanzlei
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

1. Dezember 2022

Kleine Anfrage der Abgeordneten Lisa-Marie Jeckel (Freie Wähler)
betr. Hackerangriffe und Datensicherheit im Rhein-Pfalz-Kreis
- Drucksache 18/4734 -

Die Kleine Anfrage beantworte ich namens der Landesregierung wie folgt:

Zu 1.:

Eine mögliche Beteiligung der genannten Gruppierung am Cyberangriff zum Nachteil der Kreisverwaltung des Rhein-Pfalz-Kreises ist Gegenstand laufender Ermittlungen. Bislang ist die Gruppierung in Rheinland-Pfalz nicht in Erscheinung getreten.

Zu 2. bis 4.:

Mit dem Projekt „Informationssicherheit bei den Kommunalverwaltungen in Rheinland - Pfalz“ wurde den Kommunen eine Möglichkeit gegeben, deren IT- Sicherheitsniveau zu erhöhen und somit in einen kontinuierlichen Informationssicherheitsprozess einzusteigen. Unter anderem wurde dazu ein speziell auf die Kommunalverwaltungen zugeschnittenes Profil im IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) mitentwickelt (Basis-Absicherung Kommunalverwaltung).

Auch wurde analog der Einrichtung auf Landesebene ein kommunales Computer-Emergency-Response-Team (CERT-kommunal-rlp) aufgebaut, dessen IT-Sicherheitszentrale sich bei der KommWis GmbH befindet. In enger Zusammenarbeit mit dem CERT des Landes (CERT-rlp) stehen mit dem CERT-kommunal-rlp den Kommunen IT-Sicherheitsexperten zur Verfügung, die im Rahmen eines Warn- und Informationsdienstes Informationen und Lösungsansätze anbieten sowie bei konkreten IT-Sicherheitsvorfällen koordinierend mitwirken. Weiterhin steht die Zentrale Ansprechstelle Cybercrime (ZAC) des Landeskriminalamtes Rheinland-Pfalz den hier ansässigen Unternehmen, öffentlichen sowie nichtöffentlichen Institutionen als vertrauensvoller Ansprechpartner bei der Erörterung vorbeugender Maßnahmen zur Verfügung. Dabei geht es inhaltlich vorrangig um Maßnahmen zur Steigerung von Security Awareness und weniger um technische Empfehlungen zur Härtung von IT-Systemen.

Der Verfassungsschutz Rheinland-Pfalz bietet mit der Website „cyberschutz.rlp.de“ umfangreiche Informationen rund um das Thema Schutz vor Cyberspionage und -sabotage. Das Angebot richtet sich speziell an Unternehmen und Behörden aus Rheinland-Pfalz. Auf der Website wird die Cyberbedrohungslage dargestellt und zugriffsgeschützte Informationen über sogenannte Bedrohungsindikatoren angeboten. Dabei handelt es sich um maschinenlesbare Informationen, mit denen IT-Fachleute ihre Systeme besser gegen Angriffe von außen absichern können. Sie helfen den Verantwortlichen, mit Hilfe ihrer Firewalls, Mailfilter und Sicherheitsprogramme, Infiltrationen zu erkennen. Zusätzlich werden Hinweise für den Fall eines erfolgten Cyberangriffs gegeben und die Erarbeitung von Notfallplänen empfohlen. Darüber hinaus sind auf der gemeinsamen Informationsplattform des Landes und der Kommunen „informationssicherheit.rlp“ Leitfäden des CERT-rlp verfügbar, die erforderliche Maßnahmen nach einem IT-Sicherheitsvorfall sowie Hilfestellungen zum Erkennen eines möglicherweise infizierten Systems beschreiben.

Das detaillierte Vorgehen nach einem Cyberangriff ist grundsätzlich immer in einem speziell auf die jeweilige Organisation angepassten Notfallkonzept festzulegen. Dazu bietet das Bundesamt für Sicherheit in der Informationstechnik mit seinem Standard „100-4: Notfallmanagement“ (zukünftig „200-4: Business Continuity Management“) die Grundlage. Für das Erstellen und das Fortschreiben sind die Städte, Gemeinden und Landkreise im Rahmen ihrer kommunalen Selbstverwaltung verantwortlich.

Zu 5.:

Der Landesregierung liegen keine Informationen vor, in wie vielen beziehungsweise bei welchen Kommunen in Rheinland-Pfalz entsprechende Notfallkonzepte vorliegen.

Zu 6. und 7.:

Die Ermittlung von Tatverdächtigen von Cyberangriffen stellt eine besondere Herausforderung dar, da diese regelmäßig vom Ausland aus tätig werden. Auch ist festzustellen, dass sich Hacker zu Kollektiven zusammenschließen und gemeinsam agieren. Dies vorangestellt, sind bei der Zentrale Ansprechstelle Cybercrime des Landeskriminalamtes Rheinland-Pfalz die nachfolgenden Cyberangriffe erfasst (Stichtag: 18. November 2022):

2018	**2019**	**2020**	**2021**	**2022**
75	127	81	105	130

Im Übrigen wird auf die Antwort der Landesregierung zu Frage 11 der Großen Anfrage „Cyberangriffe in Rheinland-Pfalz“ (Drucksache 18/3334) verwiesen.

Alexander Schweitzer