RheinlandPfalz
MINISTERIUM DES INNERN
UND FÜR SPORT

Ministerium des Innern und für Sport Rheinland-Pfalz
Postfach 3280 | 55022 Mainz

Präsidenten des
Landtags Rheinland-Pfalz
Herrn Hendrik Hering
Platz der Mainzer Republik 1
55116 Mainz

LANDTAG
Rheinland-Pfalz
18/6149
VORLAGE

DER MINISTER

Schillerplatz 3-5
55116 Mainz
Telefon 06131 16-0
Telefax 06131 16-3595
Poststelle@mdi.rlp.de
www.mdi.rlp.de

17. Juli 2024

Mein Aktenzeichen	Ihr Schreiben vom	Ansprechpartner/-in / E-Mail	Telefon / Fax
Bitte immer angeben!		Max Gieltowski max.gieltowski@mdi.rlp.de	06131 16-3210 06131 16-17-3210

Sitzung des Ausschusses für Digitalisierung, digitale Infrastruktur und Medien am 27. Juni 2024
TOP 6: Cybersicherheit - Sachstand Kritis-Dachgesetz und gemeinsame Sicherheitsarchitektur der Länder
Antrag der Fraktion der CDU nach § 76 Abs. 2 GOLT
- Vorlage 18/5950 -

Sehr geehrter Herr Landtagspräsident,

in der Sitzung des Ausschusses für Digitalisierung, digitale Infrastruktur und Medien am 27. Juni 2024 wurde die Übersendung des Sprechvermerks zu TOP 6 „Cybersicherheit - Sachstand Kritis-Dachgesetz und gemeinsame Sicherheitsarchitektur der Länder“ zugesagt. Ich bitte Sie, den nachfolgenden Sprechvermerk den Mitgliedern des Ausschusses für Digitalisierung, digitale Infrastruktur und Medien zu übermitteln.

Mit freundlichen Grüßen

Michael Ebling

Anlage

Sitzung des Ausschusses für Digitalisierung, digitale Infrastruktur und Medien am 27. Juni 2024
TOP 6: Cybersicherheit - Sachstand Kritis-Dachgesetz und gemeinsame Sicherheitsarchitektur der Länder
Antrag der Fraktion der CDU nach § 76 Abs. 2 GOLT
- Vorlage 18/5950 –

Die Gewissheit um die essentielle Bedeutung des Schutzes Kritischer Infrastrukturen (KRITIS) ist aufgrund der vergangenen Krisen deutlicher in den Fokus gerückt. Der Schutz von KRITIS ist eine gesamtgesellschaftliche Aufgabe, die KRITIS-Unternehmen, Verbände, Verwaltungen in Bund, Ländern und Kommunen sowie die Gesellschaft gleichermaßen betrifft. Die Thematik ist dementsprechend ein ebenen-, ressort- und akteursübergreifendes Querschnittsthema. Vor diesem Hintergrund und vor dem Hintergrund der europäischen Richtlinie über die Resilienz kritischer Einrichtungen haben die Regierungsparteien auf Bundesebene im Koalitionsvertrag vereinbart, den physischen Schutz Kritischer Infrastrukturen in einem KRITIS-Dachgesetz zu bündeln. Sektorübergreifende Mindestvorgaben für Resilienzmaßnahmen und Meldepflichten für Störungen sollen die Resilienz der Kritischen Infrastrukturen in Deutschland noch einmal erhöhen. Mit dem KRITIS Dachgesetz soll die am 16. Januar 2023 in Kraft getretene Richtlinie über die Resilienz kritischer Einrichtungen auch bekannt als CER-Richtlinie (Critical Entities Resilience Directive), umgesetzt werden. Die CER-Richtlinie gilt für kritische Einrichtungen in einer Reihe von Sektoren wie z.B. Energie, Verkehr, Bankwesen, Finanzmarktinfrastruktur, Gesundheit, Trinkwasser, Abwasser, Digitale Infrastruktur, Öffentliche Verwaltung und Weltraum. Bis Januar 2026 müssen die Mitgliedstaaten über eine nationale Strategie zur Stärkung der Resilienz kritischer Einrichtungen verfügen, mindestens alle vier Jahre eine Risikobewertung durchführen und eine Liste der kritischen Einrichtungen erstellen, die grundlegende Dienste erbringen. Die kritischen Einrichtungen wiederum müssen die relevanten Risiken ermitteln, welche die Erbringung grundlegender Dienste erheblich beeinträchtigen können; sie müssen letztlich geeignete Maßnahmen ergreifen, um ihre Resilienz zu gewährleisten und den zuständigen Behörden aufgetretene Störfälle melden. Die Richtlinie enthält auch Vorschriften zur Ermittlung kritischer Einrichtungen von besonderer europäischer Bedeutung.

Gemäß Artikel 24 der Richtlinie muss eine Umsetzung in nationales Recht bis spätestens 17. Oktober 2024 erfolgt sein. Der Bund ist derzeit noch an der Erarbeitung einer finalen Fassung eines Referentenentwurfs des KRITIS-Dachgesetzes, mit der die Länderbeteiligung fortgeführt wird. Eine Berichterstattung über die Inhalte ist vor diesem Hintergrund noch verfrüht, wenngleich sich aus Landessicht gewisse Erwartungen an ein entsprechendes Gesetz stellen. So sollte das Gesetz ein grundlegendes Regelwerk für den Schutz von Kritischen Infrastrukturen sein, das eine einheitliche KRITIS-Definition sowie Vorgaben enthält, die für Bund und Länder eine einheitliche und systematische Identifizierung von KRITIS ermöglichen. Dabei darf der Schwellenwert als eines der Identifizierungsmerkmale nicht zu hoch angesetzt werden. Maßnahmen zum Schutz von KRITIS sollen auf alle vier Phasen des Risiko- und Krisenmanagementkreislaufs ausgerichtet werden und im Gesetz definierte Standards müssen bundesweit einheitlich sein. Maßgeblich ist auch die Beibehaltung des Ressortsprinzips ohne Zuständigkeitsverlagerungen, denn der Schutz von KRITIS ist eine ressort- und akteursübergreifende sowie gesamtgesellschaftliche Aufgabe.

Im Bereich der IT-Sicherheit wurde zum Schutz von KRITS bereits früh z.B. durch das BSI-Gesetz und das IT-Sicherheitsgesetz 2.0 der gesetzliche Rahmen geschaffen, um die Resilienzen in diesem Bereich zu stärken. Auch die Umsetzung der NIS-2-Richtlinie steht derzeit an. Auf Landesebene ist das Thema Cybersicherheit, als wesentlicher Teil der gesamten Sicherheitsstruktur an folgenden Stellen fachlich verankert: Ministerium für Arbeit, Soziales, Transformation und Digitalisierung; IT-Beauftragter der Landesregierung (CIO RP); Chief Information Security Officer (CISO RP); Verfassungsschutz Rheinland-Pfalz; zentraler IT-Dienstleister des Landes (LDI RP); Computer Emergency Response Team (CERT-rlp); zentrale Ansprechstelle Cybercrime des Landeskriminalamtes (ZAC RP); Landesbeauftragter für den Datenschutz und die Informationsfreiheit (LfDI) sowie der Landeszentralstelle Cybercrime der Generalstaatsanwaltschaft (LZC).

Cybercrime ist ein hochdynamischer Kriminalitätsbereich, der die bestehenden Strukturen im Bereich IT- bzw. Cybersicherheit zu regelmäßigen Anpassungen zwingt. Um polizeilich adäquat auf diese Entwicklungen reagieren zu können, wurde die Aufbauorganisation der Polizei Rheinland-Pfalz zum 1. Juli 2024 an die sich ändernden

Rahmenbedingungen angepasst. So werden die Polizeipräsidien in den Kriminaldirektionen eigene Cybercrime-Kommissariate einrichten. Eine enge Verzahnung bzw. Zusammenarbeit zwischen den Cybercrime-Kommissariaten und dem Dezernat 47 – Cybercrime im Landeskriminalamt Rheinland-Pfalz (LKA) stärkt die Professionalität und Effizienz polizeilichen Handelns in diesem Bereich deutlich. Insbesondere die im LKA verortete Zentrale Ansprechstelle Cybercrime (ZAC) für rheinland-pfälzische Unternehmen, öffentliche und nichtöffentliche Institutionen spielt eine entscheidende Rolle. Einerseits wird eine professionelle Beratung für den Schutz von Unternehmen und Institutionen zunehmend in Anspruch genommen. Andererseits ist die qualifizierte Entgegennahme und Erst-Bearbeitung von Cyberangriffen in der ZAC für ein erfolgreiches Ermittlungsverfahren äußerst gewinnbringend.

Sowohl zur Erhöhung der Cybersicherheit als auch zur Bekämpfung von Cybercrime ist eine enge behördenübergreifende Zusammenarbeit aller staatlicher Stellen in diesem Bereich notwendig. Die Strukturen in Rheinland-Pfalz stellen dabei eine ressortübergreifende Zusammenarbeit für solche Lagen sicher. So existiert z.B. mit dem Cyber-Reaktions-Zentrum Rheinland-Pfalz (CRZ-rlp) ein interministerielles Fachgremium, das als temporäre Aufrufeinheit immer dann zum Einsatz kommt, wenn sich herausragende Cyber-Vorfälle ereignet haben. Unter dem Vorsitz des Staatssekretärs im Ministerium für Arbeit, Soziales, Transformation und Digitalisierung (MASTD) ist in diesen Fällen der unmittelbare Informationsaustausch zwischen allen beteiligten Stellen gewährleistet. Das MASTD ist darüber hinaus in Bundesgremien, wie z. B. der LAG Cybersicherheit, vertreten und stellt den Transfer über die hiesigen Strukturen sicher.

Darüber hinaus stehen Polizei und Verfassungsschutz Rheinland-Pfalz in Fällen von herausragenden Cyberangriffen unter mutmaßlicher Beteiligung staatlicher Organisationen in einem engen Informationsaustausch. Gleichzeitig weisen Verfassungsschutz und ZAC regelmäßig auf die jeweiligen präventiven Beratungsangebote der Netzwerkpartner hin.

Zwar obliegt der Schutz der jeweiligen Objekte grundsätzlich den KRITIS-Betreibern. Flankierend ergreift die Polizei gleichwohl vorbereitende Maßnahmen, um im Bedarfsfall ergänzenden Schutz gewährleisten zu können. Die einschlägigen Infrastrukturen des Landes Rheinland-Pfalz wurden hierfür erhoben und priorisiert. Je nach Bedeutung

und Gefährdung des jeweiligen Objekts kommen unterschiedliche polizeiliche Maßnahmen in Betracht, wie u. a. Aufklärungsmaßnahmen, Erstellung und Fortschreibung von Gefährdungsbewertungen, Vorhalten von Objektplänen, Sicherheitsberatungen, sowie Entwicklung denkbarer Einsatzszenarien oder formelle Schutzmaßnahmen, Polizeiintern bildet die IT-Sicherheit der polizeilichen Anwendungen insbesondere in Krisenlagen die Voraussetzung für die Funktionsfähigkeit der Polizei. Daher werden fortlaufend die technische Infrastruktur und die Schutzmechanismen geprüft. Im Rahmen von Übungen und Regelbesprechungen werden die Reaktionen bei IT-Angriffen erprobt.