



HESSISCHER LANDTAG

08. 05. 2024

Kleine Anfrage

Oliver Stirböck (Freie Demokraten)**Cyberangriffe und Cybersicherheit in Hessen vom 23.02.2024****und**

Antwort

Minister des Innern, für Sicherheit und Heimatschutz

Vorbemerkung Fragesteller:

Immer wieder werden hessische Kommunen, Unternehmen und Einrichtungen Opfer von Cyberangriffen. Zuletzt betraf es beispielsweise die Gemeinde Petersberg im Kreis Fulda. Von solchen Angriffen gehen zahlreiche Gefahren aus. Im Digitalausschuss des Landtages stand das Thema mehrfach auf der Tagesordnung. Es besteht hier dringender Handlungsbedarf. Von der neuen Landesregierung sollten weitere Impulse zur Verbesserung der Cybersicherheit ausgehen. Vor allem kleinere und mittelgroße Kommunen sind mit der Aufgabe Cybersicherheit oft überfordert.

Vorbemerkung Minister des Innern, für Sicherheit und Heimatschutz:

Die sichere und zuverlässige Verfügbarkeit der IT-Systeme und der Fachanwendungen ist für die Funktionsfähigkeit und damit die Erbringung der Dienstleistungen für die Bürgerinnen und Bürger essentiell. Den Kommunen kommt dabei aufgrund ihrer vielfältigen unmittelbaren Dienstleistungen für die Bürgerinnen und Bürger besondere Bedeutung zu.

Gemäß Artikel 28 Abs. 2 GG und Artikel 137 HV regeln die Kommunen und Landkreise in Hessen ihre Angelegenheiten (im Rahmen der bestehenden Bundes- und Landesgesetze) eigenverantwortlich und in originär eigener Zuständigkeit. Dazu zählen auch der Aufbau und die Sicherheit ihrer IT-Struktur und die Cyberresilienz insgesamt.

Die Landesregierung unterstützt und fördert die Kommunen dabei durch gezielte Angebote beim Auf- und Ausbau ihrer Cyberresilienz, da neben den allgemeinen Verwaltungsdienstleistungen oftmals auch der Betrieb von wichtigen kritischen Versorgungsdienstleistungen in der Verantwortung der Kommunen liegt.

Dazu zählen das gemeinsam mit dem zentralen kommunalen IT-Dienstleister ekom21 gegründete Kommunale Dienstleistungszentrum Cybersicherheit (KDLZ-CS) sowie das Hessische Cyberabwehrbildungszentrum Land/Kommunen (HECAAZ L/K).

Damit bietet das Land allen 442 Kommunen in Hessen die kostenfreie individuelle Beratung zur Verbesserung der Resilienz ihrer IT-Infrastruktur und IT-Systeme und Schulungsangebote.

Das CERT-Hessen des Hessen CyberCompetenceCenter (Hessen3C) im Hessischen Ministerium des Inneren, Sicherheit und Heimatschutz (HMDI) hilft Kommunen darüber hinaus bei Informationssicherheitsvorfällen über eine rund um die Uhr erreichbare Notfallnummer. Daneben unterstützt das CERT-Hessen die IT- und Informationssicherheitsbeauftragten in den Kommunen mit Services wie einem Warn- und Informationsdienst oder dem Tool Hessen Leak Checker, mit dem gestohlene Datensätze auf dienstlichen E-Mail-Adressen der teilnehmenden Kommunen und Einrichtungen der Landesverwaltung durchsucht werden (Frühwarnsystem).

Hessen3C berät und unterstützt auf Anfrage hessische Kommunen und kleine und mittlere Unternehmen sowie Betreiber kritischer Infrastrukturen in Hessen. Bei Bedarf unterstützt ein Mobile Incident Response Team (MIRT) vor Ort beim Incident-Handling und Krisenmanagement. Das MIRT ist ein mobiles Einsatzteam von IT-Experten.

Diese Vorbemerkungen vorangestellt, beantworte ich die Kleine Anfrage wie folgt:

Frage 1 Welche Erkenntnisse hat die Landesregierung bzgl. aktueller Hackerangriffe und Angriffe durch Malware gegen kommunale Einrichtungen, Behörden des Landes und private Unternehmen?

Im gesamten deutschen Cyberraum hat sich die Bedrohungslage für die Wirtschaft und öffentliche Verwaltung sowohl auf Landes- als auch Kommunalebene durch eine deutliche Zunahme von Cyberangriffen verschärft.

Grundsätzlich lassen sich sechs Haupttypen von Malware (Ransomware, Spyware, Adware, Würmer, Trojaner und Botnets) sowie vermehrt DDoS-Attacken (Distributed Denial of Service) beobachten.

Frage 2 Hat die Landesregierung Erkenntnisse darüber, welche Daten im Rahmen von Cyberattacken erbeutet wurden?

Bei der Mehrzahl der Fälle sind keine Daten abgeflossen oder Systeme komplett zum Erliegen gebracht worden.

Frage 3 Mit welchen konkreten Maßnahmen will die neue Landesregierung die Sicherheit vor Cyberangriffen in Hessen verbessern?

Frage 4 Mit welchen Maßnahmen will die Landesregierung die Schulung und Weiterbildung von Mitarbeiterinnen und Mitarbeitern der Landesverwaltung und der kommunalen Verwaltung im Bereich Cybersicherheit verbessern?

Frage 5 Plant die neue Landesregierung neue Programme zur Förderung der Cybersicherheit in Hessen?

Die Fragen 3 bis 5 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Landesregierung verfolgt das Ziel, das Hessen3C weiter zu stärken und die operativen Fähigkeiten im Sinne des Hessischen IT-Sicherheitsgesetzes weiterzuentwickeln.

Für alle Mitarbeiterinnen und Mitarbeiter der Landesverwaltung steht ein interaktives Selbstlernprogramm zur Verfügung. Zur Gewährleistung einer aktualisierten Wissensvermittlung werden die Lerninhalte fortlaufend aktualisiert und weiterentwickelt. Darüber hinaus wurden Schulungsinhalte für interaktive Schulungen zur Informationssicherheit entwickelt. Bei den Schulungsinhalten, die allen Ressorts der Landesverwaltung zur Verfügung stehen, handelt es sich u. a. um aktualitätsbezogene Hinweise zum sicheren Umgang mit den IT-Systemen. Ferner wird in Zusammenarbeit mit der Hessischen Zentrale für Datenverarbeitung (HZD) eine Fortbildung für die Informationssicherheitsbeauftragten der Landesverwaltung angeboten.

Die Landesregierung unterstützt die Kommunen durch regelmäßige Thematisierung der Bedeutung von Awareness und Prävention für den sicheren Betrieb der kommunaleigenen IT-Infrastruktur und IT-Systeme. Dies geschieht beispielsweise durch von Hessen3C durchgeführte Informationsveranstaltungen, Vorträge und Veröffentlichungen (u. a. Medien der kommunalen Spitzenverbände). Das Hessen3C führt damit kontinuierlich Informationsveranstaltungen u. a. bei Kommunen durch. In diesem Jahr wird voraussichtlich jeweils ein regionaler Cybersicherheitsgipfel in jedem der drei Regierungspräsidien stattfinden.

Die die Regierung tragenden Parteien haben in ihrem Koalitionsvertrag für die 21. Wahlperiode speziell für Kommunen ein nachhaltiges Aktionsprogramm kommunale Cybersicherheit (AKC) vereinbart, das gemeinsam mit den Kommunen aufgesetzt werden und einen konkreten Maßnahmenkatalog enthalten soll.

Frage 6 Wie plant die Landesregierung, auf die zunehmende Bedrohung durch Cyberangriffe zu reagieren und die Sicherheit der digitalen Infrastruktur des Landes insgesamt zu verbessern?

Frage 7 Welche Rolle spielt der Hessische Informationssicherheitsrat bei der Festlegung von Standards in der IT-Sicherheit der Landesverwaltung?

Die Fragen 6 und 7 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Das Hessische Gesetz zum Schutz der elektronischen Verwaltung (HITSiG) enthält umfassende Rechtsgrundlagen für die Aufgaben und Befugnisse des Hessen3C als Zentrum für Informationssicherheit. Zudem wurde die Position des Chief Information Security Officer (CISO) gesetzlich verankert. Die Umsetzung des HITSiG stellt somit eine wichtige Grundlage für die Erhöhung der Informations- und Cybersicherheit und zur Abwehr von Gefahren für die Informationstechnik des Landes dar. Eine Weiterentwicklung aus Anlass der stetig steigenden Anforderungen zur Sicherung der Cyber- und Informationssicherheit der Landesverwaltung ist beabsichtigt.

Mit der Einrichtung eines Informationssicherheitsrates, der die Standards in der IT-Sicherheit festlegen soll, und durch die Anhebung des Schutzbedarfes der zentralen Infrastrukturen, dem Einsatz vertrauenswürdiger IT sowie dem Ausbau des zentralen Landes-IT-Dienstleisters soll die Cyberresilienz gesteigert werden.

Frage 8 Wie plant die Landesregierung die hessische Verwaltung an den Mindeststandard des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu orientieren?

Die Landesverwaltung orientiert sich an den BSI-Standards. Eine landesseitige Konkretisierung erfolgt durch das Hessische IT-Sicherheitsgesetz (HITSiG) und die aktuell gültige Hessische Informationssicherheitsleitlinie.

Frage 9 Beabsichtigt die neue Landesregierung das Thema Cybersicherheit besser institutionell innerhalb der Landesverwaltung und der kommunalen Verwaltung zu verankern?

Aus Sicht der Landesregierung stellt auf kommunaler Ebene die Aufgabenwahrnehmung der Cybersicherheit durch qualifiziertes Fachpersonal die strategisch wichtigste Institutionalisierung dar. Hierzu wirbt die Landesregierung bei den kommunalen Verwaltungsleitungen dafür, diese wichtige Aufgabe durch hauptamtliche IT-Sicherheitsbeauftragte (ITSB) wahrnehmen zu lassen. Die Erfahrung zeigt, dass die Aufgabenwahrnehmung durch einen hauptamtlichen ITSB, der sich ausschließlich um die IT-Sicherheit kümmert, zu einem spürbar höheren Resilienzniveau der kommunalen IT-Infrastruktur führt.

Dabei unterstützt die Landesregierung kommunale Initiativen beispielsweise auf Kreisebene (ITSB für Kreisverwaltung und kreisangehörige Kommunen) oder der gemeinsamen Aufgabenwahrnehmung mehrerer Kommunen auf Grundlage der Förderung der interkommunalen Zusammenarbeit auch finanziell.

Wiesbaden, 29. April 2024

Prof. Dr. Roman Poseck