



HESSISCHER LANDTAG

29. 01. 2020

Kleine Anfrage

Dr. h.c. Jörg-Uwe Hahn (Freie Demokraten), Stefan Müller (Freie Demokraten) und Oliver Stürböck (Freie Demokraten) vom 08.11.2019

Hessen3C – Cybersicherheit und Sicherheitsbehörden

und

Antwort

Minister des Innern und für Sport

Vorbemerkung Fragesteller:

Hessen3C soll die zentrale Kompetenzstelle zur interdisziplinären Zusammenarbeit und Kooperation staatlicher Behörden in Hessen sein. Es hat die Aufgabe, die Sicherheit in der Informationstechnik des Landes zu erhöhen, cyberspezifische Gefahren abzuwehren, die Effizienz der Bekämpfung der Cyberkriminalität zu erhöhen und Synergien zu schaffen. Bestandteil der Aufgaben ist der regelmäßige Informationsaustausch mit der Hessischen Polizei und dem Hessischen Verfassungsschutz sowie die Erstellung eines gemeinsamen Lagebildes für Hessen. Das solle unter Beibehaltung der jeweiligen Zuständigkeiten und unter strikter Wahrung des Trennungsgebotes zwischen Polizei und Verfassungsschutz erfolgen.

Vorbemerkung Minister des Innern und für Sport:

Das Hessen Cyber Competence Center (Hessen3C) wurde am 8. April 2019 offiziell eröffnet und nach abgeschlossener Pilotphase im September 2019 als Referat in die Regelorganisation der Abteilung VII „Cyber- und IT-Sicherheit, Verwaltungsdigitalisierung“ des Hessischen Ministeriums des Innern und für Sport überführt.

Das Hessen3C ist die zentrale Kompetenzstelle zur interdisziplinären Zusammenarbeit und Kooperation zwischen hessischen Sicherheitsbehörden, Verwaltung und Wissenschaft. Aufgabe des Hessen3C ist es, die Effizienz bei der Abwehr cyberspezifischer Gefahren und der Bekämpfung von Cyberkriminalität unter weitgehender Ausnutzung von Synergien zu erhöhen.

Das Alleinstellungsmerkmal des Hessen3C ist die Bündelung von Fachkompetenz in den Bereichen Cybersecurity, Cyberintelligence und Cybercrime und der dadurch erst - unter Wahrung des Trennungsgebots - mögliche Informationsaustausch über Behördengrenzen hinweg. Der durch Hessen3C neu geschaffene regelmäßige Lageaustausch zwischen den Bereichen Cybersecurity, Cybercrime und Cyberintelligence, dem Hessischen Landeskriminalamt und dem Landesamt für Verfassungsschutz Hessen ermöglicht es, Schwachstellen, Angriffe und aktuelle Kriminalitätsphänomene im Cyberbereich effizient und umfassend zu bewerten sowie zielgerichtete und abgestimmte Maßnahmen einzuleiten.

Mit dem Hessen3C wurde ein zentraler Ansprechpartner in allen cyberbezogenen Angelegenheiten etabliert, der sowohl den Schutz der Cybersicherheit in der Landesverwaltung, die Unterstützung der Sicherheitsbehörden bei der Ausbildung von Expertinnen und Experten, der Bekämpfung von Cybercrime und Cyberspionage als auch die Beratung von Kommunen, Unternehmen und Betreibern Kritischer Infrastrukturen (KRITIS) zum Auftrag hat. Das Hessen3C ist gemäß BSI-Gesetz zentrale Meldestelle für hessische KRITIS-Unternehmen. Zudem können durch das im Hessen3C eingerichtete Mobile Incident Response Team (MIRT) Unternehmen im Falle eines Cyberangriffes vor Ort unterstützt und erste Erkenntnisse zu dem vorliegenden Sachverhalt forensisch gesichert werden. Für die hessische Landes- und Kommunalverwaltung sowie für Kleine und Mittlere Unternehmen in Hessen steht mit dem Hessen3C ein an sieben Tagen in der Woche und rund um die Uhr erreichbarer, zentraler Ansprechpartner bei Cybersicherheitsvorfällen im Land Hessen bereit, der mit hoher fachlicher Kompetenz berät.

Das Beratungs- und Informationsangebot des Hessen3C richtet sich aber auch an Bürgerinnen und Bürger. Nutzer mobiler Endgeräte können sich über die App „hessenWARN“ aktuelle Meldungen des Hessen3C eventuell relevanten Spam-Wellen oder neuen Angriffsvarianten auf Computer oder

Netzwerke anzeigen lassen. Auch im Rahmen des jährlich vom Hessischen Ministerium des Innern und für Sport als öffentliche Fachveranstaltung durchgeführten Cybersicherheits-Gipfels leistet das Hessen3C einen zentralen Beratungs- und Informationsbeitrag.

Auch der im Januar 2019 bekannt gewordene Doxing-Fall (nicht autorisierte Veröffentlichung von personenbezogenen Daten im Netz, z.B. Adress- und Kontodaten von Politikerinnen und Politikern) hat gezeigt, dass Träger eines politischen Mandats Ziel von Cyberangriffen sein können. Hessen3C konnte hier durch seine zentral gebündelte Kompetenz eine schnelle Einschätzung vornehmen, unmittelbar reagieren, die Betroffenen persönlich informieren und maßgeblich zur Eingrenzung der Folgen beitragen. Im September 2019 hat das Hessen3C zudem eine Awareness-Veranstaltung für Abgeordnete und Mitarbeiterinnen und Mitarbeiter des Hessischen Landtags durchgeführt.

Über diese Kernaufgaben hinaus fungiert das Hessen3C zudem als Geschäftsstelle der Länderoffenen Arbeitsgruppe Cybersicherheit (LOAG) der Innenministerkonferenz und bringt sich maßgeblich in die Beratungen des Nationalen Cybersicherheitsrats (NCSR) ein. Damit setzt das Hessen3C wichtige Impulse und trägt zur strategischen Ausrichtung der Cybersicherheit und zur Stärkung der Rolle des Landes Hessen im Bund-Länder-Kontext bei. Hessen3C betreibt in Zusammenarbeit mit der Zentralstelle zur Bekämpfung der Internetkriminalität der Generalstaatsanwaltschaft Frankfurt (ZIT) die Meldestelle im Meldesystem Hessen gegen Hetze.

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

Frage 1. Wie viele Anfragen auf konkrete Unterstützung und Beratung sind bisher von Seiten hessischer Unternehmen beim H3C eingegangen?

Seit der Eröffnung von Hessen3C am 08.04.2019 sind seitens hessischer Unternehmen 16 Anfragen (Stand: 15.01.2020) auf konkrete Unterstützung und Beratung eingegangen.

Über die konkrete Unterstützung und Beratung aufgrund von Anfragen hinaus stellt Hessen3C auch Referentinnen und Referenten für Fachveranstaltungen der Industrie- und Handelskammern, der Handwerkskammern, Verbänden oder Unternehmen aus dem Bereich der Kritischen Infrastrukturen.

Zu den Beratungs- und Unterstützungsleistungen im weiteren Sinne zählt auch die Durchführung eigener Veranstaltungen für Kleine und Mittlere Unternehmen, etwa auch für die Zielgruppe der kommunalen Unternehmen; zuletzt etwa die Fachtagung „Der große Blackout – IT-Sicherheit und Krisenvorsorge zum Schutz Kritischer Infrastrukturen“, die Hessen3C in Kooperation mit der Abteilung Brand- und Katastrophenschutz des HMdIS, dem Verband der kommunalen Unternehmen (Hessen) und dem Landesverband der Energie und Wasserwirtschaft (Hessen und Rheinland-Pfalz) veranstaltet hat.

Frage 2. Wie viele Anfragen auf konkrete Unterstützung und Beratung sind bisher seitens der Kommunen beim H3C eingegangen?

Seit der Eröffnung von Hessen3C am 08.04.2019 sind seitens hessischer Kommunen 20 Anfragen (Stand: 15.01.2020) auf konkrete Unterstützung und Beratung eingegangen und bearbeitet worden. Zudem wurde eine Vielzahl telefonischer Beratungen durchgeführt und spezifische Rückfragen telefonisch oder per E-Mail beantwortet.

Darüber hinaus werden folgende Leistungen für die Kommunen angeboten:

- Der Warn- und Informationsdienst für die Kommunen. Die Nutzung ist für die Kommunen kostenlos und freiwillig. Der Warn- und Informationsdienst informiert über gefährliche Schwachstellen und Sicherheitslücken sowie über aktuelle Bedrohungslagen und erreicht unmittelbar ca. 30 Kommunen direkt und mittelbar über den kommunalen Dienstleister ekom21 mehr als 90 % der hessischen Kommunen.
- Vorträge eigener Referentinnen und Referenten bei Veranstaltungen mit der Zielgruppe Kommunen, Beteiligung an der eXPO (Hausmesse der ekom21), auf dem Hessentag sowie Präsenz auf unterschiedlichen Messen.
- Organisation, Durchführung und inhaltliche Vorbereitung der Sitzungen des Arbeitskreises Kommunale Cybersicherheit der Kommunalen Spitzenverbände.
- Einbindung der Kommunen bei Übungen und Awareness-Maßnahmen, wie beispielsweise Phishing-Tests für die Landesverwaltung.
- Mit dem vom Hessen3C betreuten Förderprogramm „Kommunales Dienstleistungszentrum Cybersicherheit“ (KDLZ-CS) wird den hessischen Kommunen zudem der Einstieg in ein Informationssicherheitsmanagement erleichtert. Dazu gehören eine standardisierte Erhebung des

Ist-Zustandes der Informationssicherheit in der Kommune, ein eLearning-Programm „Informationssicherheit“ für die Beschäftigten der teilnehmenden Kommune und eine Empfehlung zur Verbesserung der Informationssicherheit (Maßnahmen-Plan). Das Programm begann 2016 und ist bis Ende 2021 mit insgesamt 8,17 Mio. € finanziert. Bisher wurden 327 Kommunen durch das KDLZ-CS beraten (Stand: 03.01.2020).

Frage 3. Ist das H3C mit seinen Fachprozessen in einem Informationssicherheitskonzept nach BSI betrachtet worden?

Das Hessen3C betreibt derzeit keine eigenen Fachverfahren. Daher wurden bisher auch keine IT-Sicherheitskonzepte nach BSI-Grundschrift/ISO 2700x erstellt. Gleichwohl wurde eine BSI-Zertifizierung für das Hessen3C eingeleitet. Aktuell basiert die Arbeit des Hessen3C auf den allgemeinen vom Land bereitgestellten Lösungen.

Frage 4. Verfügen die Hessische Polizei, das Landeskriminalamt (LKA) und das Hessische Landesamt für Verfassungsschutz (LfV) über ein aktuelles Informationssicherheitskonzept nach BSI oder ISO 2700x?

Bei der hessischen Polizei existiert eine Informationssicherheitsleitlinie (ISLL, Stand 31.10.2016). Diese gilt für alle hessischen Polizeidienststellen, das LKA und die Hochschule für Polizei und Verwaltung (HfPV). Neben dieser Leitlinie gibt es das „Handbuch zur IT-Sicherheit bei der hessischen Polizei“, welches Regelungen einer Sicherheitsrichtlinie beinhaltet und im Zusammenhang mit der Neuregelung des BSI-Grundschriftkompendiums aktualisiert wird. Darüber hinaus gibt es in den hessischen Polizeidienststellen weitere Dokumente mit Bezug zur IT-Sicherheit in Form von Dienstanweisungen, Richtlinien und Leitfäden.

Das Landesamt für Verfassungsschutz Hessen verfügt derzeit über kein Informationssicherheitskonzept nach BSI oder ISO 2700x. Die Organisationseinheit „Online Recherche Team Terrorismus und Extremismus“ (ORTET) hat ein solches Konzept für die dort entwickelten Fachverfahren erstellt. Die anderen in der Behörde verwendeten Fachverfahren sind Dienstleistungen der Hessischen Zentrale für Datenverarbeitung, des Bundeskriminalamtes sowie des Bundesamtes für Verfassungsschutz. Gleichwohl beabsichtigt das Landesamt für Verfassungsschutz Hessen zukünftig für die Gesamtheit der eingesetzten Fachverfahren eine Dokumentation nach BSI-Grundschrift.

Wiesbaden, 28. Januar 2020

Peter Beuth