20. Wahlperiode

Drucksache **20/8293**

HESSISCHER LANDTAG

20. 06. 2022

Kleine Anfrage

Stefan Müller (Heidenrod) (Freie Demokraten), Dr. Stefan Naas (Freie Demokraten) und Oliver Stirböck (Freie Demokraten) vom 12.04.2022

Stärkung der Cybersicherheit in Unternehmen

und

Antwort

Minister des Innern und für Sport

Vorbemerkung Fragesteller:

Mit Hessen3C, dem CyberCompetenceCenter, hat die hessische Landesregierung eine Einheit geschaffen, die sowohl Behörden als auch kleine und mittelständische Unternehmen dabei unterstützt, Cyberattacken mit Beratungsmaßnahmen vorzubeugen und bei Cyberattacken mit Abwehrmechanismen zu unterstützen. Hessen3C leistet damit einen wichtigen Beitrag zur Sicherheit von Computersystemen des Landes, der Kommunen und von Unternehmen. Insbesondere kleine Unternehmen und auch Mittelständler sind jedoch oftmals aufgrund personeller Bedürfnisse nicht nur mit der fachlichen Umsetzung überfordert. Auch die finanziellen Erfordernisse einer angemessenen technischen Umsetzung verlangt Unternehmen viel ab. Mit dem wachsenden Bedürfnis von Beschäftigten nach mobilem Arbeiten steigen auch die Anforderungen an die IT-Sicherheit von Systemen, die nun nicht mehr nur Angriffe auf einen Standort, sondern auf viele dezentrale Geräte abwehren können müssen. Das Bundeskriminalamt vermeldet daher auch im jährlichen Bundeslagebild Cybercrime wachsende Fallzahlen und begründet dies auch mit einer steigenden Anzahl an Tatgelegenheiten und zunehmender Professionalisierung. In einer repräsentativen Befragung des Branchenverbands BITKOM melden deutsche Unternehmen im Jahr 2021 eine Gesamtschadenssumme von 223,5 Mrd. Euro durch Datendiebstahl, Industriespionage und Sabotage. Die finanziellen Schäden haben sich damit gegenüber dem Vorjahr mehr als verdoppelt. Aus diesen Steigerungsraten ergeben sich verschiedene Verpflichtungen. Einerseits liegt es an Unternehmen, sich mit der Frage auseinanderzusetzen, wie Daten und Systeme ausreichend geschützt und aktuell gehalten werden können und wie sie ihre Beschäftigten schulen können, um den Einfluss des Faktors Mensch in der Gefährdung der IT-Sicherheit zu verringern. Allerdings liegt es offensichtlich im Interesse von Unternehmen, diese Schritte umzusetzen. Wichtig ist auch, ein stärkeres Bewusstsein für IT-Sicherheit zu schaffen, in der Bevölkerung sowie in Unternehmen
Da die Integrität der IT-Systeme auch im Interesse des Staates liegt, ist auch die Herstellung von Cybersicherheit eine Aufgabe, die der Staat zumindest unterstützen sollte

Die Vorbemerkung der Fragesteller vorangestellt, beantworte ich die Kleine Anfrage im Einvernehmen mit dem Minister für Wirtschaft, Energie, Verkehr und Wohnen wie folgt

Frage 1. Inwiefern sieht die Landesregierung eine Verantwortung bei sich, im Dienste der Gesamtintegrität von IT-Systemen, die IT-Sicherheit von Unternehmen finanziell zu unterstützen?

Frage 2. Welche Möglichkeiten bietet die Landesregierung für kleine und mittlere Unternehmen, um sich die Verstärkung der IT-Sicherheit mit Fördermitteln des Landes Hessen fördern zu lassen?

Frage 3. Welche einzelbetrieblichen Angebote bietet die Landesregierung für kleine und mittlere Unternehmen konkret, um sich hinsichtlich der IT-Sicherheit beraten zu lassen?

Die Fragen 1 bis 3 werden aufgrund ihres Sachzusammenhangs zusammen beantwortet.

Die Hessische Landesregierung erachtet Cyber- und IT-Sicherheit als besonders wichtig. Dementsprechend stellt sie zur Erhöhung der IT-Sicherheit ein umfangreiches Unterstützungsangebot für staatliche und nichtstaatliche Organisationen sowie Akteure zur Verfügung.
Das Land Hessen bietet kleinen und mittleren Unternehmen (KMU) eine breite Palette an Unterstützungsangeboten zur Sicherung und Stärkung ihrer Wettbewerbsfähigkeit. Die Erhöhung der IT-Sicherheit in den Unternehmen hat in diesem Rahmen eine hohe Bedeutung.
Mit dem Förderprogramm DIGI-Zuschuss unterstützt das Land Hessen KMU der gewerblichen Wirtschaft und Freie Berufe bei der konkreten Einführung neuer digitaler Systeme sowie der Verbesserung der IT-Sicherheit. Der Zuschuss beträgt bis zu 10.000 € bei einem Fördersatz von bis zu 50 %. Im Rahmen einer Befragung geförderter Unternehmen gaben 36 % an, dass die

Eingegangen am 20. Juni 2022 · Ausgegeben am 22. Juni 2022
Herstellung: Kanzlei des Hessischen Landtags · Postfach 3240 · 65022 Wiesbaden · www.Hessischer-Landtag.de

Erhöhung der IT- oder Datensicherheit bei der Beantragung des DIGI-Zuschuss für sie als Ziel im Vordergrund stand.
Für größere Projekte steht das Förderprogramm „digital jetzt“ des Bundesministeriums für Wirtschaft und Klimaschutz zur Verfügung. Dieses fördert unter anderem auch Investitionen in digitale Technologien, welche die IT-Sicherheit und den Datenschutz erhöhen. Hier beträgt die maximale Fördersumme für einzelne Unternehmen bis zu 50.000 €.
Neben allgemeinen Existenzgründungs- und Betriebsberatungen werden KMU auch spezifische Digitalisierungsberatungen angeboten. Diese umfassen neben der Digitalisierung von Geschäftsprozessen, Produkten und Dienstleistungen auch Fragen der IT-Sicherheit und des Datenschutzes. KMU stehen hier sowohl das branchenoffene Beratungsangebot der RKW Hessen GmbH als auch ein branchenspezifisches Angebot speziell für das Handwerk seitens der drei hessischen Handwerkskammern zur Verfügung, um ihre individuellen Fragestellungen zu klären.
Hessen3C im Hessischen Ministerium des Innern und für Sport bietet KMU niederschwellig kostenlose fachliche Beratungen an. Diese reichen von Beratungen zur Absicherung der IT-Infrastruktur, zu Maßnahmen zur Notfallvorsorge und -planung (Business Continuity Management) über Präventions- und Awareness-Veranstaltungen bis hin zur Unterstützung in konkreten IT-Sicherheitsvorfällen. Bisher führte Hessen3C 67 solche Beratungsveranstaltungen für KMU auf deren Anfrage durch.
Zur Unterstützung bei akuten IT-Sicherheitsvorfällen erreichen alle hessischen KMU das Hessen3C über dessen rund um die Uhr besetzte Hotline. KMU werden bei der konkreten Vorfallsanalyse, dem Incident-Handling und Krisenmanagement unterstützt. Mit einem Mobile Incident Response Team (MIRT) hilft Hessen3C bei Bedarf auch landesweit vor Ort.
Hessen3C stellt im Weiteren einen Warn- und Informationsdienst als Newsletter zur Verfügung, der insbesondere über aktuelle Cyber-Bedrohungen informiert, so dass frühzeitig erforderliche Abwehrmaßnahmen umgesetzt werden können.

Frage 4. Wie viele Unternehmen haben seit Einrichtung von Hessen3C welche Dienste des Centers in Anspruch genommen?

Seit seiner Einrichtung im April 2019 haben sich 187 KMU mit der Bitte um Unterstützung oder Beratung an das Hessen3C gewandt. Die Unterstützungsbedarfe bezogen sich sowohl auf konkrete Sicherheitsvorfälle wie Ransomware-Angriffe als auch auf Beratungen und Informationen zu allgemeinen Fragenstellungen im Kontext der IT- und Cybersicherheit. Eine differenzierte Erfassung einzelner Unterstützungsleistungen erfolgt insoweit nicht. Den Warn- und Informationsdienst haben derzeit 70 hessische KMU abonniert.

Frage 5. In wie vielen Fällen konnte Hessen3C seit Einrichtung bei akuten Sicherheitsvorfällen eines Unternehmens unterstützen?

Es wird auf die Antwort zur Frage 4 verwiesen.

Frage 6. Wie groß ist der wirtschaftliche Schaden durch Cyberangriffe in den Jahren 2019 bis 2021 in Hessen gewesen? (Bitte nach Jahren einzeln auflisten.)

Hessen3C erhält im Rahmen seiner Unterstützungsleistungen für KMU keine Kenntnis über durch Cyberangriffe verursachte Schäden. Auch darüber hinaus liegen der Hessischen Landesregierung hierzu keine validen Informationen vor.

Frage 7. Wie schätzt die Landesregierung die Gefahr für hessische Unternehmen durch russische Cyberangriffe im Zuge des russischen Angriffskriegs auf die Ukraine ein?

Aufgrund des russischen Angriffskriegs gegen die Ukraine besteht gegenwärtig eine erhöhte Bedrohungslage für Deutschland und damit auch für Hessen. Die Gefahren bestehen insbesondere dadurch, dass der Krieg durch verschiedenste Formen von Cyberangriffen flankiert wird. Hieraus resultiert die Gefahr einer möglichen Betroffenheit durch Kollateralschäden. Über wechselseitige Cyberangriffe der Kriegsparteien könnte sich z. B. Schadsoftware über Lieferketten im Bereich Software auch nach Deutschland und Hessen ausbreiten. Darüber hinaus besteht die Möglichkeit gezielter russischer Cyberangriffe gegen kritische Infrastrukturen in Deutschland als Vergeltung für westliche Sanktionen und die Unterstützung der Ukraine. Hinzu kommen eine besondere Volatilität, ausgelöst durch auf beiden Seiten der Kriegsparteien agierende nichtstaatliche Akteure und die Ausnutzung der aktuellen Lage durch allgemeinkriminelle Cybergruppierungen.

Wiesbaden, 1. Juni 2022

Peter Beuth