Landtag von Baden-Württemberg **Drucksache 17 / 2250**

17. Wahlperiode **29.3.2022**

Kleine Anfrage

des Abg. Dr. Reinhard Löffler CDU

und

Antwort

des Ministeriums des Inneren, für Digitalisierung und Kommunen

Cyberangriffe auf baden-württembergische Unternehmen

Kleine Anfrage

Ich frage die Landesregierung:

1. Wie viele Cyberangriffe auf Unternehmen in Baden-Württemberg wurden seit 2018 bis 2021 den entsprechenden Behörden zur Kenntnis gebracht (mit der Bitte um Aufschlüsselung nach Schadsoftware/Malware, Ransomware, DDoS-Angriffe, Backdoor-Angriffe, Advanced Persistent Threads und Social Engineering)?

2. Wie hoch schätzt sie die Dunkelziffer solcher Attacken ein?

3. Wie hoch werden die materiellen Schäden dieser Angriffe in besagtem Zeitraum beziffert (aufgeschlüsselt nach Art der Angriffe)?

4. Ist die Zahl der Cyberangriffe nach Einschätzung der Landesregierung durch vermehrtes Homeoffice vieler Angestellter seit Beginn der Covid-19-Pandemie signifikant gestiegen?

5. Unternehmen sind laut Datenschutz-Grundverordnung (DSGVO) nur zur Meldung beim Landesbeauftragten für den Datenschutz und Informationsfreiheit Baden-Württemberg verpflichtet, falls sich ein Cyberangriff auf personenbezogene Daten ausgewirkt hat – ist besagte Dienststelle der Bearbeitung dieser gewachsen?

6. Ist die Landesregierung der Ansicht, dass im Hinblick auf eine rapide Ausbreitung von Cyberattacken die besagte Meldepflicht noch ausreichend ist oder sollte diese auf weitere als lediglich personenbezogene Daten ausgeweitet werden?

7. Inwiefern ist ihrer Ansicht nach die gegründete Cybersicherheitsagentur Baden-Württemberg (CSBW) in der Lage, digitale Einbruchsversuche in der Breite wirkungsvoll einzudämmen?

Eingegangen: 29.3.2022 / Ausgegeben: 12.5.2022

8. Hält es die Landesregierung für zielführend, zum Aufbau einer Agentur zur Abwehr und Analyse von Cyberangriffen von Nutzern von Computern und Telekommunikationseinheiten eine Transaktionsabgabe zu verlangen, die von den Providern „eingesammelt“ wird?

9. Soweit eine Transaktionsabgabe nicht in Betracht kommen sollte – würde die Landesregierung eine Pauschalabgabe für den Cyberschutz für Speichermedien und IT-Endgeräte befürworten, vergleichbar der GEMA-Abgabe für Speichermedien und IT-Endgeräte, zur Finanzierung für den Aufbau einer Agentur zur Abwehr und Analyse von Cyberangriffen?

29.3.2022

Dr. Löffler CDU

Begründung

Wirksamer Schutz gegen Cyberangriffe kann nur eine Agentur leisten, die mit erheblichen Geldmitteln ausgestattet ist, damit eine wirksame Infrastruktur aufgebaut und kompetente Mitarbeiter eingestellt werden. Aus Haushaltsmittel ist das schwerlich zu leisten und kann effizient mit einer Abgabe, entweder als Transaktionsabgabe oder als Pauschalabgabe auf Speichermedien und IT-Endgeräte finanziert werden. Im Gegensatz zur GEMA-Abgabe wird dies auch die Unterstützung der Nutzer finden, da diese einen wirksamen Schutz erfahren, der bislang nicht gewährleistet ist. Da nicht nur Unternehmen und Privatpersonen Opfer von Hackerangriffen sind, sondern zunehmend auch öffentliche Einrichtungen, ist der Aufbau einer solchen Agentur dringend erforderlich. Die Höhe von Transaktionskosten und Pauschalabgabe ist minimal. „Die Masse macht’s“.

Antwort

Mit Schreiben vom 21. April 2022 Nr. IM7-0141-27/13/2 beantwortet das Ministerium des Inneren, für Digitalisierung und Kommunen im Einvernehmen mit dem Ministerium für Wirtschaft, Arbeit und Tourismus die Kleine Anfrage wie folgt:

1. Wie viele Cyberangriffe auf Unternehmen in Baden-Württemberg wurden seit 2018 bis 2021 den entsprechenden Behörden zur Kenntnis gebracht (mit der Bitte um Aufschlüsselung nach Schadsoftware/Malware, Ransomware, DDoS-Angriffe, Backdoor-Angriffe, Advanced Persistent Threads und Social Engineering)?

2. Wie hoch schätzt sie die Dunkelziffer solcher Attacken ein?

3. Wie hoch werden die materiellen Schäden dieser Angriffe in besagtem Zeitraum beziffert (aufgeschlüsselt nach Art der Angriffe)?

Zu 1. bis 3.:

Die statistische Erfassung von Straftaten erfolgt bei der Polizei Baden-Württemberg anhand der Polizeilichen Kriminalstatistik (PKS). Bei der PKS handelt es sich um eine sogenannte Ausgangsstatistik, in der strafrechtlich relevante Sachverhalte nach der polizeilichen Sachbearbeitung vor Abgabe an die Strafverfolgungsbehörden erfasst werden. Die Fallerfassung erfolgt nach den bundeseinheitlichen „Richtlinien für die Führung der Polizeilichen Kriminalstatistik“. Eine ge-

sonderte Erfassung von Cyberangriffen auf Unternehmen ist in der PKS nicht vorgesehen. Vor diesem Hintergrund können keine belastbaren Aussagen im Sinne der Fragestellungen getroffen werden. Anhand der in der PKS insgesamt erfassten Straftaten im Deliktsbereich Cybercrime kann allerdings festgestellt werden, dass dieses Deliktsfeld seit mehreren Jahren von kontinuierlichen Fallzahlenanstiegen geprägt ist. Im Jahr 2021 wurde mit insgesamt 10 744 erfassten Fällen im Bereich Cybercrime ein weiterer Anstieg im Vergleich zum Jahr 2020 mit 10 248 Fällen verzeichnet. Der größte Anteil entfällt mit 8 152 Fällen im Jahr 2021 auf Delikte des Computerbetrugs. Eine besonders deutliche Steigerung ist bei den Delikten der Datenveränderung und Computersabotage mit 63 Prozent auf insgesamt 326 Fälle festzustellen. Auch die Fälle des Ausspähens und Abfangens von Daten stiegen im Jahr 2021 um rund 25 Prozent auf 1 046 Fälle im Vergleich zum Vorjahr.

Das Landesamt für Verfassungsschutz Baden-Württemberg (LfV) erhielt für den erfragten Zeitraum Hinweise im unteren dreistelligen Bereich zu Cyberangriffen mit mutmaßlich nachrichtendienstlichem Hintergrund. Zum Ausmaß der tatsächlichen Schäden durch Cyberspionage oder Cybersabotage liegen dem LfV indes keine belastbaren Zahlen vor.

Das Innenministerium geht von einem großen Dunkelfeld im Bereich der Cyberkriminalität aus. Diese Einschätzung resultiert zum einen aus der Erkenntnis, dass Angriffe im Internet von Betroffenen häufig nicht bemerkt werden. Dies kann daran liegen, dass die Angriffe durch technische Sicherungsmechanismen automatisch verhindert werden. Auch können Informationstechnik oder Daten der Geschädigten unbemerkt zur Begehung weiterer Cyberangriffe missbraucht werden. Letzteres ist beispielsweise der Fall, wenn die Angreifer die Informationstechnik der Geschädigten missbräuchlich als Teil eines Bot-Netzes zur Durchführung von Distributed-Denial-of-Service (DDoS)-Angriffen nutzen. Zum anderen werden Straftaten in diesem Bereich oftmals auch nicht zur Anzeige gebracht. Dies ist insbesondere dann der Fall, wenn Geschädigten vermeintlich kein finanzieller Schaden entstanden ist oder dieser von Dritten reguliert wird. Insbesondere bei Wirtschaftsunternehmen wird das Anzeigeverhalten auch durch die Angst vor etwaigen Reputationsverlusten negativ beeinflusst.

Einen Anhaltspunkt zur Quantifizierung des Dunkelfeldes im Bereich der Cyberkriminalität bietet der Cyber-Security-Risk-Report 2021 der MHP Management- und IT-Beratung GmbH, welcher in Kooperation mit dem Landeskriminalamt Baden-Württemberg (LKA) erstellt wurde. Von den im Rahmen der Studie befragten Unternehmen gab nahezu die Hälfte an, innerhalb der vergangenen zwei Jahre Geschädigter eines Delikts im Bereich der Cyberkriminalität geworden zu sein. Andere Studien, beispielsweise des Branchenverbands BITKOM e. V. und des Kriminologischen Forschungsinstituts Niedersachsen, kommen bei ähnlichen Fragestellungen zu vergleichbaren Ergebnissen.

Im Übrigen wird auf die Stellungnahme zu den Ziffern 1 bis 3 des Antrags der Abgeordneten Daniel Karrais u. a. FDP/DVP (Drucksache 17/483) verwiesen.

4. Ist die Zahl der Cyberangriffe nach Einschätzung der Landesregierung durch vermehrtes Homeoffice vieler Angestellter seit Beginn der Covid-19-Pandemie signifikant gestiegen?

Zu 4.:

Die Coronapandemie, die zum Teil gravierend veränderte Arbeitsbedingungen zur Folge hatte, trug in den vergangenen zwei Jahren zu einer deutlichen Erhöhung der Gefahren für die Cybersicherheit bei. Die Aufrechterhaltung von etablierten IT-Sicherheitsstandards, gerade auch in häuslichen Umgebungen und beim mobilen Arbeiten, stellte Sicherheitsverantwortliche mitunter vor große Herausforderungen.

Angreifer beobachten stets neue Gegebenheiten und passen ihre Angriffstaktiken und -strategien daran an, um ihre Ziele zu attackieren. Nach einer Umfrage des Branchenverbands BITKOM e. V. und darauf basierenden Berechnungen des Ins-

tituts der deutschen Wirtschaft Köln e. V. waren in Deutschland im Jahr 2020 allein 52,5 Milliarden Euro an Schäden auf Angriffe im Homeoffice zurückzuführen. Ein Anstieg von 25,7 Prozent (31 Milliarden Euro) im Vergleich zum Jahr 2019 – lässt sich danach auf die Arbeit im Homeoffice zurückführen.

Im Übrigen wird auf die Stellungnahme zu Ziffer 8 des Antrags der Abgeordneten Daniel Karrais u. a. FDP/DVP (Drucksache 16/8662) verwiesen.

5. Unternehmen sind laut Datenschutz-Grundverordnung (DSGVO) nur zur Meldung beim Landesbeauftragten für den Datenschutz und Informationsfreiheit Baden-Württemberg verpflichtet, falls sich ein Cyberangriff auf personenbezogene Daten ausgewirkt hat – ist besagte Dienststelle der Bearbeitung dieser gewachsen?

Zu 5.:

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LfDI) Baden-Württemberg ist eine unabhängige, oberste Landesbehörde und nicht Teil der Landesregierung. Der LfDI wurde angefragt, beteiligt sich jedoch grundsätzlich nicht an der Beantwortung von Anfragen von Abgeordneten des Landtags durch die Landesregierung.

Der LfDI nimmt wahr, dass die vom Ukrainekrieg ausgelösten Fragen zur Sicherheit und zum Schutz (personenbezogener) Daten verschiedene Akteure in Politik und Wirtschaft beschäftigen. Diese Fragen wird der LfDI im Rahmen seines Kompetenzbereichs beantworten und die Verantwortlichen bei der Evaluation und erforderlichenfalls der Anpassung des Datenschutzmanagements unterstützen.

Zudem ist beim LfDI eine Veranstaltung gemeinsam mit den Sicherheitsbehörden in Planung, um die Abgeordneten und die Beschäftigten des Landtags kurzfristig im Rahmen einer Informationsveranstaltung aufzuklären.

6. Ist die Landesregierung der Ansicht, dass im Hinblick auf eine rapide Ausbreitung von Cyberattacken die besagte Meldepflicht noch ausreichend ist oder sollte diese auf weitere als lediglich personenbezogene Daten ausgeweitet werden?

Zu 6.:

Über die Meldepflicht gegenüber dem LfDI nach Artikel 33 der Datenschutz-Grundverordnung hinaus bestehen für Betreiber Kritischer Infrastrukturen, Anbieter digitaler Dienste und Unternehmen im besonderen öffentlichen Interesse bereits heute Meldepflichten, die nicht auf die Meldung bei der Verletzung des Schutzes personenbezogener Daten begrenzt sind, vgl. etwa § 8b Absatz 4, § 8c Absatz 3 und § 8f Absatz 7 des BSI-Gesetzes. So sind diese Betreiber und Anbieter etwa zu einer Meldung verpflichtet, wenn es zu erheblichen IT-Störungen oder Ausfällen kommt.

Es wird erwartet, dass der Kreis meldepflichtiger Unternehmen mit der sich aktuell in den Trilog-Verhandlungen zwischen EU-Parlament und Rat im Beisein der EU-Kommission befindlichen Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union („NIS 2“) eine deutliche Erweiterung erfährt.

7. Inwiefern ist ihrer Ansicht nach die gegründete Cybersicherheitsagentur Baden-Württemberg (CSBW) in der Lage, digitale Einbruchsversuche in der Breite wirkungsvoll einzudämmen?

Zu 7.:

Die nachhaltige Stärkung der Cybersicherheit erfordert eine enge Zusammenarbeit aller relevanten Akteure auf diesem Gebiet. Ziel ist es, die Cybersicherheit in Baden-Württemberg stetig zu verbessern. Mit der im Dezember 2021 von der Landesregierung verabschiedeten Cybersicherheitsstrategie Baden-Württemberg – Perspektive 2026 – und der damit einhergehenden neuen Cybersicherheitsarchitektur im Land soll die von der Landesregierung formulierte Vision, dass Menschen, Staat, Wirtschaft und Wissenschaft die Chancen der Digitalisierung ohne erhebliche Gefährdungen durch Cyberangriffe nutzen können, Wirklichkeit werden. Ziel dieser ganzheitlichen Cybersicherheitsstrategie ist eine Verbesserung des allgemeinen Cybersicherheitsniveaus, das alle gesellschaftlichen Bereiche umfasst. Für diese Zielerreichung treten auf Seiten der Sicherheitsbehörden nicht nur die Cybersicherheitsagentur Baden-Württemberg, sondern auch das LKA und das LfV ein.

Im Übrigen wird auf die Stellungnahme zu Ziffer 5 des Antrags der Abgeordneten Daniel Karrais u. a. FDP/DVP (Drucksache 17/483) und die Antworten auf die Fragen 3 bis 5 der Kleinen Anfrage des Abgeordneten Fabian Gramling CDU (Drucksache 16/7847) verwiesen.

8. Hält es die Landesregierung für zielführend, zum Aufbau einer Agentur zur Abwehr und Analyse von Cyberangriffen von Nutzern von Computern und Telekommunikationseinheiten eine Transaktionsabgabe zu verlangen, die von den Providern „eingesammelt“ wird?

9. Soweit eine Transaktionsabgabe nicht in Betracht kommen sollte – würde die Landesregierung eine Pauschalabgabe für den Cyberschutz für Speichermedien und IT-Endgeräte befürworten, vergleichbar der GEMA-Abgabe für Speichermedien und IT-Endgeräte, zur Finanzierung für den Aufbau einer Agentur zur Abwehr und Analyse von Cyberangriffen?

Zu 8. und 9.:

Mit Fortschreiten der Digitalisierung nehmen auch die Risiken und Gefährdungspotenziale zu, die im Zusammenhang mit dem Einsatz neuer, digitaler Technologien stehen. Hierzu zählen u. a. auch Cyberangriffe. Die Cyber- und Informationssicherheit betrifft Staat, Wirtschaft und Gesellschaft gleichermaßen. Auf Seiten der Wirtschaft treffen die Unternehmen – entsprechend ihrer jeweiligen Risikodisposition und -bewertung – eigene Vorkehrungen, um möglichen Schäden durch Cyberangriffe vorzubeugen und wenden hierzu eigene Mittel auf. Die Wirtschaft trägt zudem auch z. B. durch die Entwicklung innovativer technischer Lösungen wesentlich zur Gefahrenabwehr bei.

Zur Gewährleistung eines hohen Niveaus an Cybersicherheit ist aber auch der Staat auf Ebene des Bundes und der Länder in einer besonderen Verantwortung. Dies umfasst die Übernahme grundlegender und übergreifender Maßnahmen, etwa zur Abwehr von Cyberangriffen, aber auch zur Prävention oder im Rahmen der Strafverfolgung.

Die Finanzverfassung des Grundgesetzes geht davon aus, dass der allgemeine Finanzbedarf des Staates aus Steuern gedeckt wird („Prinzip des Steuerstaates“). Steuern sind gemäß § 3 Absatz 1 der Abgabenordnung „Geldleistungen, die nicht eine Gegenleistung für eine besondere Leistung darstellen und von einem öffentlich-rechtlichen Gemeinwesen zur Erzielung von Einnahmen allen auferlegt werden, bei denen der Tatbestand zutrifft, an den das Gesetz die Leistungspflicht knüpft.“

Bei einer Sonderabgabe handelt es sich dagegen um eine Abgabe, der keine zurechenbare Gegenleistung gegenübersteht, die aber im Unterschied zu Steuern nicht von der Gesamtheit der Steuerbürgerinnen und -bürger, sondern nur von einer bestimmten Gruppe erhoben wird und zur Finanzierung besonderer Aufgaben dient. Sonderabgaben sind nach der gefestigten Rechtsprechung des Bundesverfassungsgerichts eigenständige, nichtfiskalische Abgaben. Da Sonderabgaben gegenüber der Steuerfinanzierung die seltene Ausnahme bleiben sollen, bedürfen sie einer besonderen verfassungsrechtlichen Rechtfertigung. So dürfen Sonderabgaben nur eine vorgefundene homogene Gruppe belasten. Dabei muss u. a. zwischen dem mit der Abgabenerhebung verfolgten Zweck und dieser Gruppe eine spezifische Sachnähe, d. h. eine Finanzierungsverantwortung, bestehen. Hieran dürfte es bei einer Transaktions- oder Pauschalgabe zum Aufbau einer Agentur zur Abwehr und Analyse von Cyberangriffen fehlen. Denn Cybersicherheit betrifft alle Bürgerinnen und Bürger. Allein in Deutschland wird es laut der globalen, regionalen und länderspezifischen Studie „Cisco Annual Internet Report“ bereits im Jahr 2023 ca. 823 Millionen vernetzte Geräte geben. Insoweit dürfte es bereits an einer homogenen Gruppe fehlen, welche zur Finanzierungsverantwortung gezogen würde.

In Vertretung

Klenk

Staatssekretär