MINISTERIUM FÜR INNERES, DIGITALISIERUNG UND MIGRATION
B A D E N - W Ü R T T E M B E R G

Postfach 10 34 65 • 70029 Stuttgart
E-Mail: poststelle@im.bwl.de
FAX: 0711/231-5000

An die
Präsidentin des Landtags
von Baden-Württemberg
Frau Muhterem Aras MdL
Haus des Landtags
Konrad-Adenauer-Str. 3
70173 Stuttgart

Datum 22.01.2021

nachrichtlich
Staatsministerium
Ministerium für Finanzen
Ministerium für Wissenschaft, Forschung und Kunst
Ministerium für Umwelt, Klima und Energiewirtschaft

Kleine Anfrage des Abgeordneten Nico Weinmann FDP/DVP
- Hackerangriff auf „Solarwinds“ und Auswirkungen auf Baden-Württemberg
- Drucksache 16/9556
Ihr Schreiben vom 18. Dezember 2020

Sehr geehrte Frau Landtagspräsidentin,

das Ministerium für Inneres, Digitalisierung und Migration beantwortet die Kleine Anfrage im Einvernehmen mit dem Ministerium für Finanzen, dem Ministerium für Wissenschaft, Forschung und Kunst und dem Ministerium für Umwelt, Klima und Energiewirtschaft wie folgt:

1. *Gehörten oder gehören Behörden, Organisationen, sonstige öffentliche Einrichtungen des Landes Baden-Württemberg (Ministerien, obere und untere Landesbehörden, Polizei und Justiz, Hochschulen, Forschungseinrichtungen, kritische Infrastrukturen) oder öffentlich-rechtliche Körperschaften zu den Kunden des US-amerikanischen Netzwerksicherheitsanbieters „Solarwinds“, der jüngst Opfer eines globalen Hacker-Angriffs wurde und nutzten dabei die von Hackern manipulierte Version der Solarwinds-Software „Orion“, wenn ja, welche?*

2. *Konnten die Hacker hierdurch Zugriff auf sicherheitsrelevante Daten, vertrauliche Dokumente, Verschlusssachen und persönliche Korrespondenzen erlangen?*

3. *Wenn ja, in welchem Umfang wurden tatsächlich durch die zum Spionageprogramm manipulierte Software „Orion“ entsprechende Datensätze „abgegriffen“ unter Darlegung, wie groß die Landesregierung die sich hieraus ergebenden Gefahren einschätzt?*

Zu 1., 2. und 3.:

Die von der Sicherheitslücke betroffene Software „Orion" des amerikanischen Netzwerksicherheitsanbieters SolarWinds ist in den Behörden, Organisationen und sonstigen öffentlichen Einrichtungen des Landes Baden-Württemberg nicht im Einsatz. Daher sind in diesen Einrichtungen auch keine entsprechenden Sicherheitsvorfälle zu verzeichnen. Auch den baden-württembergischen Sicherheitsbehörden liegen keine Erkenntnisse im Sinne der Fragestellungen vor.

4. *Welche Sicherheitsmaßnahmen wurden zur Prävention des Angriffs in den betroffenen Behörden und Einrichtungen getroffen?*

5. *Welche Konsequenzen zieht die Landesregierung aus dem Hackerangriff hinsichtlich des künftigen Cybersicherheits-Managements der betroffenen Landesbehörden und Einrichtungen, insbesondere bei der Auswahl von Netzwerksicherheitsdienstleistern, bei Prüfung und Monitoring von verwendeter Software?*

Zu 4. und 5.:

Sowohl bei der IT Baden-Württemberg (BITBW) als zentralem IT-Dienstleister der Landesverwaltung als auch beim Landeszentrum für Datenverarbeitung (LZfD) der Oberfinanzdirektion Karlsruhe sind umfassende Maßnahmen zur Prävention und Erkennung entsprechender Hackerangriffe umgesetzt und werden laufend fortentwickelt. Dies ist vor dem Hintergrund des stetigen Fortschritts der technologischen Entwicklungen und der sich beständig ändernden Rahmenbedingungen und Angriffsvektoren ein auf Dauer angelegter, kontinuierlicher Prozess.

Die Einrichtung des Sicherheitszentrum IT in der Finanzverwaltung Baden-Württemberg (SITiF BW) beim LZfD zur weiteren Verbesserung der Informationssicherheit in der gesamten Finanzverwaltung und die Neukonzeption des CERT BWL im Rahmen der geplanten Errichtung einer Cybersicherheitsagentur zu einer zentralen Stelle für präventive und reaktive Maßnahmen in der gesamten Landesverwaltung sind hier besonders hervorzuheben.

Mit dem von der Landesregierung am 17. Dezember 2020 in den Landtag eingebrachten Gesetzentwurf zur Verbesserung der Cybersicherheit und Änderung anderer Vorschriften wird das zukünftige Cybersicherheits-Management der öffentlichen Stellen des Landes weiter zusammengeführt und entscheidend fachlich und methodisch gestärkt. Wichtige Elemente hierbei sind die zentrale Steuerung der Abwehr von Gefahren für die Cybersicherheit, die Einrichtung einer zentralen Koordinierungs- und Meldestelle für Sicherheitsvorfälle, die Entwicklung, Setzung und Überprüfung von Sicherheitsstandards für die öffentlichen Stellen des Landes sowie die Unterstützung dieser Stellen bei deren Umsetzung. Der Cybersicherheitsagentur soll darüber hinaus die Befugnis eingeräumt werden, auf dem Markt bereitgestellte Produkte und Systeme auf ihren sicheren Einsatz in der Landesverwaltung hin zu untersuchen und zu bewerten.

Bei Ausschreibungen und vor dem Einsatz von Hard- und Software prüfen die IT-Dienstleister der Landesverwaltung bereits heute, ob Hersteller und deren Lösungen nationale oder internationale Sicherheitsstandards einhalten. Als geeignete Nachweise dienen beispielsweise Zulassungen und Zertifikate des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und Common Criteria-Zertifikate. Bei der Beauftragung Externer werden im Sinne einer Dienstleistersteuerung nach den Maßgaben der BSI-Standards hohe Anforderungen an deren Vertraulichkeit gestellt. Das Erfüllen von Sicherheitsvorgaben wird bereits in den Anforderungskatalogen der entsprechenden

Ausschreibungen berücksichtigt, entsprechende Vereinbarungen fließen in die Verträge mit den Dienstleistern und Lieferanten ein.

6. *Welche Unternehmen und privaten Einrichtungen in Baden-Württemberg, insbesondere im Bereich der „kritischen Infrastrukturen“, sind ihr bekannt, die vom betreffenden Hackerangriff auf die Software der Firma „Solarwinds“ betroffen sind?*

Zu 6.:

Den baden-württembergischen Sicherheitsbehörden liegen keine Erkenntnisse über von einem entsprechenden Hackerangriff betroffene Unternehmen und private Einrichtungen vor.

Zum Rechtsrahmen für die IT-Sicherheit Kritischer Infrastrukturen und den daraus resultierenden Vorgaben für Meldepflichten von Sicherheitsvorfällen wird auf die Antwort zu den Ziffern 1 und 2 der vorangegangenen Großen Anfrage „IT-Sicherheit von Kritischer Infrastruktur (KRITIS) und Institutionen im besonderen staatlichen Interesse (INSI)“ der FDP/DVP-Fraktion (Drucksache 16/3345) verwiesen.

Meldepflichten bestehen demnach für Betreiber Kritischer Infrastrukturen im Sinne des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG) in Verbindung mit der Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) nur gegenüber dem BSI.

Den zuständigen Ressorts der Landesverwaltung liegen ebenfalls keine Informationen über Unternehmen oder private Einrichtungen im Bereich KRITIS aus Baden-Württemberg vor, die vom „SolarWinds“-Hackerangriff betroffen waren. Insbesondere seitens der zu den KRITIS zählenden Universitätsklinika des Landes wurde kein Sicherheitsvorfall in diesem Zusammenhang gemeldet.

7. *Sind nach ihrer Kenntnis Städte und Gemeinden in Baden-Württemberg und deren kritische Infrastrukturen (Stadtwerke, kommunale Krankenhäuser etc.) vom „Solarwinds“-Hackerangriff betroffen?*

Zu 7.:

Den baden-württembergischen Sicherheitsbehörden liegen keine Erkenntnisse über Städte und Gemeinden bzw. kritische Infrastrukturen vor, die vom „Solar-Winds“-Hackerangriff betroffen sind.

Die Ausgestaltung ihrer jeweiligen IT-Infrastrukturen obliegt den Kommunen im Rahmen der kommunalen Selbstverwaltung. Meldeverpflichtungen, auch hinsichtlich der der Anfrage zu Grunde liegenden Thematik, gibt es für Kommunen gegenüber der Landesverwaltung derzeit keine. Dennoch stehen das Ministerium für Inneres, Digitalisierung und Migration und BITBW mit der Komm.ONE als zentralem IT-Dienstleister der Kommunen und dem dort angesiedeltem Cyber Security Incident Response Teams (CSIRT) zu Themen der IT- und Informationssicherheit in regelmäßigem fachlichen Austausch. Eine entsprechende Anfrage bei Komm.ONE ergab, dass Komm.ONE selbst keine Komponenten der Software „Orion“ des Herstellers SolarWinds einsetzt und damit ebenfalls von dem Vorfall nicht betroffen ist. Im Rahmen der kommunalen Selbstverwaltung werden in vielen Kommunen auch IT-Dienste in eigener Hoheit und Verantwortung betrieben. Komm.ONE und der Landesverwaltung liegen bislang keine Informationen über eine weitere kommunale Betroffenheit vor.

Mit dem Gesetzentwurf zur Verbesserung der Cybersicherheit und dem Aufbau der Cybersicherheitsagentur Baden-Württemberg sollen entsprechende verbindliche Melde- und Reaktionswege auch zwischen Land und Kommunen etabliert werden.

8. *Welche Erkenntnisse liegen den Strafverfolgungs- und Justizbehörden des Landes Baden-Württemberg derzeit im Zusammenhang mit Ermittlungen über den „Solarwind“-Hackerangriff vor?*

Zu 8.:

Die Polizei Baden-Württemberg führt derzeit kein Ermittlungsverfahren im Sinne der Fragestellung.

Das Bundeskriminalamt teilte am 23. Dezember 2020 mit, im Auftrag der Generalstaatsanwaltschaft Frankfurt am Main ein Ermittlungsverfahren in diesem Zusammenhang zu führen. In diesem Rahmen prüft das Bundeskriminalamt aktuell die Übernahme einer zentralen Ermittlungsführung.

9. *Liegen ihr nach gegenwärtigem Stand Erkenntnisse zu Tätern oder Verdächtigen im Zusammenhang mit dem Hackerangriff vor, etwa zu möglichen Verbindungen nach Baden-Württemberg?*

Zu 9.:

Der Polizei Baden-Württemberg liegen im Zusammenhang mit dem Hackerangriff aktuell keine Erkenntnisse zu Tätern, Tatverdächtigen oder möglichen Bezügen nach Baden-Württemberg vor.

Aus Sicht des Landesamtes für Verfassungsschutz (LfV) lassen die hohe technische Professionalität des Angreifers sowie die Art, die Methodik und der Umfang des aktuellen „SolarWinds“-Cyberangriffs eher auf einen staatlichen Akteur schließen. Konkrete Belege dafür existieren bis dato allerdings nicht – auch nicht zu der in der öffentlichen Berichterstattung explizit unterstellten Verbindung zu russischen Nachrichtendiensten.

10. *Welche Maßnahmen unternahmen die Sicherheitsbehörden des Landes ab dem Zeitpunkt der Kenntnisnahme der oben abgefragten Vorfälle?*

Zu 10.:

Die Landesverwaltung Baden-Württemberg steht über den Verwaltungs-CERT-Verbund mit den CERTs des Bundes und der Länder und mit dem BSI in einem stetigen und schnellen Austausch. Eine Kenntnisnahme von solchen Ereignissen und die Warnung vor potentiellen Gefahren erfolgt daher auf Fachebene sehr frühzeitig und dadurch auch vor einer Veröffentlichung in den Medien.

Die zentralen IT-Dienstleister und Informationssicherheitsbeauftragten der Landesverwaltung haben unverzüglich nach Eingang einschlägiger Warnmeldungen die Betroffenheit der in ihrem Verantwortungsbereich liegenden Dienststellen und Einrichtungen geprüft. Da im Ergebnis keine Betroffenheit festgestellt werden konnte, waren speziell in Bezug auf die veröffentlichte Sicherheitslücke der Software „Orion“ von SolarWinds keine dedizierten technischen Maßnahmen notwendig. Die Gesamtsituation wurde und wird jedoch mit erhöhter Aufmerksamkeit weiter beobachtet.

Am 11. Dezember 2020 und damit ebenfalls sehr frühzeitig und deutlich vor der medialen Berichterstattung veröffentlichte das Landeskriminalamt Baden-Württemberg (LKA), Zentrale Ansprechstelle Cybercrime (ZAC), eine Warnmeldung zum Cyberangriff auf den US-amerikanischen IT-Security-Konzern „FireEye“. Das Unternehmen war von der SolarWinds-Kompromittierung direkt betroffen und stellte im Dezember 2020 unautorisierte Netzwerkzugriffe und Datenabflüsse fest. Durch FireEye dokumentierte Indikatoren zur Detektion einer eventuell unbemerkt gebliebenen Kompromittierung sind inhaltlicher Bestandteil der Warnmeldung des LKA. Die Warnmeldung wurde als Pressemitteilung des LKA sowie über die Sozialen Medien veröffentlicht. Weiterhin erfolgte eine Steuerung der Warnmeldung über den Warnmeldungsverteiler der ZAC.

Die Cyberabwehr des LfV hat die bis zum 15. Dezember 2020 verfügbaren Informationen zum Angriff analysiert und mit Warnmeldung vom 16. Dezember 2020 sowohl auf die mögliche Bedrohung baden-württembergischer Behörden und Unternehmen durch diesen Cyberangriff hingewiesen als auch entsprechende Hinweise und Handlungsempfehlungen gegeben. Diese Warnmeldung wurde inzwischen an mehr als 900 Unternehmen, Verbände, Behörden und weitere Stellen verteilt. Relevante Rückmeldungen zum Sachverhalt stehen bisher aus.

Die Spionage- und Cyberabwehr sowie der Wirtschaftsschutz des LfV stehen zudem in engem Kontakt und Austausch mit dem Bundesamt für Verfassungsschutz (BfV), anderen Verfassungsschutzbehörden der Länder, dem BSI sowie der Polizei.

Darüber hinaus hat das BSI nach eigenen Angaben sämtliche ihm bekannte und betroffene Kunden des Unternehmens SolarWinds im deutschen Raum kontaktiert und gewarnt.

Mit freundlichen Grüßen

gez. Thomas Strobl
Minister für Inneres, Digitalisierung und Migration