

**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

Datum 07.03.2019

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

nachrichtlich

Staatsministerium

Ministerium für Wirtschaft, Arbeit und Wohnungsbau

Antrag der Abgeordneten Nico Weinmann u. a. FDP/DVP

- Spionage und Zugriff auf die Infrastruktur des Landes - Wie geht die Landesregierung mit Bedenken aus Sicherheitskreisen um?
- Drucksache 16/5709

Ihr Schreiben vom 14. Februar 2019

Sehr geehrte Frau Landtagspräsidentin,

das Ministerium für Inneres, Digitalisierung und Migration nimmt im Einvernehmen mit dem Ministerium für Wirtschaft, Arbeit und Wohnungsbau zu dem Antrag wie folgt Stellung:

*Der Landtag wolle beschließen,
die Landesregierung zu ersuchen*

zu berichten,

1. *inwieweit öffentliche Infrastruktur, Dienste und behördliche Ausstattungen in Baden-Württemberg auf Produkte von Huawei oder zu Huawei gehörenden Organisationen zurückgreifen;*

Zu 1.:

In der Landesverwaltung sind insbesondere Internet-Access-Router (ca. 70 Stück) und mobile Internet-Access-Surfsticks (ca. 3300 Stück) sowie wenige Smartphones, Videokonferenzsysteme und Tablets der Firma Huawei im Einsatz. Die Geräte dienen der Herstellung von Internetzugängen, überwiegend für den Einsatz bei Außenprüfungen in der Finanzverwaltung. Die hierüber eingerichtete Datenübertragung erfolgt verschlüsselt und wird damit als ausreichend sicher erachtet.

Im Rechenzentrum der BITBW und in den lokalen Netzwerken (LAN) sind keine Geräte von Huawei in Verwendung.

2. *inwieweit sie der Ansicht ist, dass es in Baden-Württemberg Sicherheitsrisiken beim Einsatz von Huawei-Produkten gibt beziehungsweise geben könnte;*

Zu 2.:

Bezüglich der derzeit in der Landesverwaltung verwendeten Huawei-Geräte werden keine Sicherheitsrisiken gesehen, insbesondere weil keinerlei Abhängigkeit der Funktionsfähigkeit der IT-Systeme der Landesverwaltung von den verwendeten Geräten besteht und der Datenaustausch über Verbindungen, die über Internet-Access-Geräte zu IT-Systemen der Landesverwaltung aufgebaut werden, verschlüsselt erfolgt.

Generell gilt, dass bei der Beschaffung bzw. der Durchführung von Vergabeverfahren von den jeweiligen Bietern das Erfüllen von definierten Kriterien gefordert wird. Die Einhaltung bzw. Erfüllung von solchen Kriterien und Standards hat der Anbieter entsprechend nachzuweisen. In derlei Fällen ist es möglich, das Bundesamt für Sicherheit in der Informationstechnik (BSI) oder andere externe Experten zu einer Beurteilung hinzuzuziehen.

3. *welche Prüfungen möglicher Sicherheitsrisiken beim Einsatz von Huawei-Produkten in ihrem Verantwortungsbereich bisher erfolgt sind;*
4. *inwieweit daran das Landesamt für Verfassungsschutz, die Cyberwehr, das Landeskriminalamt und andere Behörden des Landes beteiligt waren;*

Zu 3. und 4.:

An zentralen Stellen der IT-Infrastruktur der Landesverwaltung kommen wie unter Ziffer 1. erläutert keine Produkte von Huawei zum Einsatz. Wie unter Ziffer 1 und 2 dargelegt erfolgt die Datenübertragung bei Verwendung von Huawei-Internet-Access-Geräten (Router und Surfsticks) verschlüsselt. Die Beurteilung der Sicherheit von IT-Produkten im Zuge von Beschaffungsprozessen erfolgt bei kritischen Komponenten unter anderem anhand der vom BSI zur Verfügung gestellten Listen über vom BSI geprüfte und zertifizierte Hardware. In Bereichen, in denen ein Einsatz BSI zertifizierter oder zugelassener Lösungen beispielsweise in Ermangelung solcher Zertifikate nicht möglich ist, erfolgt eine Prüfung anhand eigener Kompetenzen und Erfahrungen in Abstimmung mit dem BSI oder ggf. unter Hinzuziehung Externer.

Das Landesamt für Verfassungsschutz Baden-Württemberg (LfV) führt keine anlassunabhängigen technischen Produktprüfungen durch. Bei der Verwendung von technischen Erzeugnissen im amtlichen Verschlusssachenwesen stützt sich das LfV – im Einklang mit dem Vorgehen des Verfassungsschutzverbundes – ebenfalls auf die Prüfung, Freigabe oder Zertifizierung durch das BSI. Zu entsprechenden Prüfergebnissen von Huawei-Produkten liegen dem LfV keine Erkenntnisse vor, da ein Einsatz von Huawei-Produkten in diesem Bereich bislang nicht vorgesehen war.

Die Polizei Baden-Württemberg lässt ebenfalls besondere Sorgfalt bei der Wahl der einzusetzenden Hardwarekomponenten walten. Dazu gehört insbesondere beim Umgang mit als Verschlusssachen eingestuften Daten entsprechende Produkte einzusetzen, deren Sicherheit durch das BSI in Form einer Zertifizierung bestätigt wurde. Wo solche Produkte nicht am Markt zur Verfügung stehen, werden grundsätzlich gesonderte Verträglichkeitsprüfungen durchgeführt.

Die Cyberwehr als Pilotprojekt im Raum Karlsruhe für kleinere und mittlere Unternehmen zur Unterstützung bei Cybersicherheitsvorfällen ist an solchen Prüfungen nicht beteiligt.

5. *inwieweit sie dabei im Austausch mit Bundesbehörden stand beziehungsweise steht;*

Zu 5.:

Bei der Risikoanalyse und der Umsetzung von Maßnahmen im Kontext der Informationssicherheit orientiert sich die Landesverwaltung an den einschlägigen BSI-Standards und an vom BSI vorgenommenen Prüfungen und erteilten Zertifikaten für Anwendungen und Systeme. Hierbei steht das Innenministerium in regelmäßigem fachlichen Austausch mit dem BSI. Durch die jüngst erfolgte Ansiedlung des BSI-Verbindungsbüros Süd in Stuttgart wird diese Zusammenarbeit weiter gestärkt.

In der im Auftrag des IT-Planungsrates arbeitenden AG Informationssicherheit spricht sich die Landesregierung mit anderen Bundesländern und dem BSI sowie Vertretern des Bundesinnenministeriums zu aktuellen Themen der Informationssicherheit ab. Gleiches gilt für die ebenfalls unter Mitwirkung der Landesregierung agierende „Länderoffene Arbeitsgruppe Cybersicherheit der Innenministerkonferenz“, in die die aktuellen Diskussionen ebenfalls einfließen.

Im Bereich der Spionageabwehr liegt die zentrale Auswertungskompetenz beim Bundesamt für Verfassungsschutz (BfV). Der Kontakt zum BSI ist im Bereich der Spionageabwehr über das BfV gegeben.

6. *inwieweit sie die Sicherheitsbedenken des ehemaligen Präsidenten des Bundesnachrichtendienstes, Gerhard Schindler, teilt, wonach die Beteiligung am 5G-Netzausbau dazu führen könne, dass Menschen rechtswidrig abgehört werden können;*

7. *inwieweit sie die Bedenken aus Sicherheitsbehörden teilt, wonach Huawei bei einer Beteiligung am 5G-Netz in der Lage wäre, das Netz in Deutschland abzuschalten;*

8. *inwieweit sie die Bedenken aus Sicherheitsbehörden teilt, wonach Unternehmen durch Huawei bzw. chinesische Stellen ausspioniert werden könnten;*

Zu 6. bis 8.:

Zu den tatsächlichen Möglichkeiten des potentiellen Abhörens oder eines Abschaltens des 5G-Netzes kann die Landesregierung insbesondere auf Grund der technischen

Komplexität dieses Spezialgebietes zum jetzigen Zeitpunkt nicht abschließend Stellung nehmen. Dies betrifft im 5G-Netz auch die Beurteilung möglicher, im IT-Umfeld etablierter Schutzmaßnahmen wie der Einsatz von Verschlüsselung und die Schaffung von Redundanzen. Hier ist auch zu berücksichtigen, dass im 5G-Umfeld die Standardisierung und Ausarbeitung der technischen Spezifikationen noch nicht abgeschlossen ist.

Das BSI hat auf Anfrage der Landesregierung mitgeteilt, dass derzeit keine konkreten Erkenntnisse vorliegen, die einen Ausschluss von Huawei-Produkten rechtfertigen würden. Dementsprechend hat sich das BSI öffentlich zunächst weiterhin gegen einen Bann von Huawei-Produkten ausgesprochen. Sollte sich die Erkenntnislage ändern, würde auch das BSI seine Haltung aktualisieren.

Die Landesregierung wird sich zu diesem Themenkomplex weiterhin und fortlaufend mit dem BSI austauschen.

9. *welche Bedeutung und Folgen derartige Bedenken für ihr Handeln haben;*

Zu 9.:

Wie bereits unter Ziff. 1. bis 4. dargestellt finden an zentralen Stellen in der IT-Landschaft der Landesverwaltung derzeit keine Geräte der Firma Huawei Verwendung.

Die Landesregierung hat im Bundesrat ihre Unterstützung zu einem umfangreichen Maßnahmenpaket der EU zur Bekämpfung von Cyberangriffen und zum Aufbau einer starken Cybersicherheit in der EU ausgesprochen. So ist im Zuge der Einigung über den „Rechtsakt zur Cybersicherheit“ in der EU unter anderem geplant, einen EU-weit geltenden europäischen Zertifizierungsrahmen für die Cybersicherheit von Produkten, Verfahren und Diensten zu schaffen.

Die aktuelle Situation macht aber auch deutlich, dass Bürgerinnen und Bürger sowie Firmen in Baden-Württemberg eine qualifizierte Beratung zum Einsatz von technischen Kommunikationskomponenten benötigen, um Risiken und Chancen in eigener Entscheidungsfreiheit abwägen zu können. Mit dem Ausbau bestehender

Beratungsangebote im Zuge der von Innenminister Strobl zum Thema Cybersicherheit angekündigten Sensibilisierungskampagne, mit der Etablierung der Cyberwehr und mit der jüngst erfolgten Ansiedlung eines BSI-Verbindungsbüros in Stuttgart sind wichtige Schritte hierfür bereits erfolgt.

Gefahren durch Spionage stellen ein abstraktes Gefährdungsmoment für Staaten, Sicherheitsbehörden, andere Stellen und die Wirtschaft dar. Aus diesem Grund werden Informationen hinsichtlich geheimdienstlicher Agententätigkeiten fremder Staaten innerhalb der Sicherheitsbehörden analysiert. Auf Bundesebene erfolgt dies u. a. im Rahmen des Gemeinsamen Extremismus- und Terrorismusabwehrzentrums Spionage/Proliferation (GETZ SP) in Köln. Auf Landesebene wird von Polizei und Verfassungsschutz die „Gemeinsame Informations- und Analysestelle Spionage“ betrieben. Die Ergebnisse werden den Bedarfsträgern aus Polizei und Nachrichtendiensten im Rahmen der gesetzlichen Möglichkeiten zur Verfügung gestellt.

Für den Bereich der Wirtschaftsspionage wurde in den vergangenen vier Jahren gemeinsam mit dem Max-Planck-Institut für ausländisches und internationales Strafrecht Freiburg sowie dem BKA das Forschungsprojekt „Wirtschaftsspionage und Konkurrenzausspähung in Deutschland und Europa“ (WISKOS) durchgeführt. Die Ergebnisse werden Unternehmen, dem Hochschul- und Forschungsbereich sowie den Polizeien der Länder und des Bundes zur Verfügung gestellt.

Im Zuge von Sensibilisierungen und bei Präventionsberatungen geht das LfV regelmäßig auf die möglichen Risiken von Spionageaktivitäten ein, verweist gleichzeitig aber auch auf fehlende Belege für tatsächliche Manipulationen von Auftragsnehmern und Auftragsbeteiligten.

Aufgrund der herausragenden Bedeutung der Cybersicherheit im Zeitalter der Digitalisierung und des steigenden Gefahrenpotentials durch Cyberangriffe erarbeitet die Landesregierung derzeit eine Cybersicherheitsstrategie für Baden-Württemberg.

- 10. inwieweit sie die Einschätzung des Grünen-Innenpolitikers Konstantin von Notz teilt, wonach die Bundesregierung das Gefahrenpotenzial in dieser Sache komplett negiert;*

Zu 10.:

Der Landesregierung ist die hohe und wachsende Bedeutung der Cybersicherheit bewusst, was sich in den unter Ziff. 9. aufgelisteten Aktivitäten widerspiegelt. Auch der Bund, mit dem das Land wie unter Ziff. 3., 4. und 5. eng zusammenarbeitet, misst der Cybersicherheit einen hohen Stellenwert bei.

- 11. ob sie es in diesem Zusammenhang für ausreichend erachtet, wenn Huawei oder die chinesische Regierung zusichern, dass nicht spioniert oder abgeschaltet wird;*
- 12. wie sie die dahingehende Aussage von Bundeskanzlerin Dr. Merkel anlässlich ihres Japanbesuchs mit Blick auf Baden-Württemberg bewertet;*
- 13. ob sie der Ansicht ist, dass man in zentralen Fragen der deutschen Sicherheit – und damit auch der Sicherheit von Baden-Württemberg – allein den Versprechungen eines anderen, nichtdemokratischen Staates vertrauen sollte;*
- 14. welche Konsequenzen sie aus dieser Überzeugung zieht.*

Zu 11. bis 14.:

Da die Landesregierung, wie unter Ziff. 1., 3. und 4. erläutert, keine Produkte von Huawei in neuralgischen bzw. sicherheitsrelevanten Bereichen einsetzt, ist die Frage nach der Wertung entsprechender Zusicherungen gegenstandslos. Zudem wird auf die Ziff. 2. und die entsprechenden Ausführungen zu Beschaffung und Ausschreibungen verwiesen.

Mit freundlichen Grüßen
in Vertretung des Ministers

gez. Julian Würtenberger
Staatssekretär