



HESSISCHER LANDTAG

27. 03. 2024

Kleine Anfrage

Oliver Stirböck (Freie Demokraten) vom 23.02.2024

Cybersicherheit in Bezug auf China und chinesische Technologieunternehmen und Antwort

Minister des Innern, für Sicherheit und Heimatschutz

Vorbemerkung Fragesteller:

Die Europäische Kommission hat die Konzerne Huawei und ZTE als Risiko für die Sicherheit der EU eingestuft. Beide Unternehmen sind am Aufbau von 5G-Netzen in Deutschland beteiligt.

Diese Vorbemerkung des Fragestellers vorangestellt, beantworte ich die Kleine Anfrage im Einvernehmen mit der Ministerin für Digitalisierung und Innovation wie folgt:

- Frage 1 Welche Auswirkungen hat nach Ansicht der Landesregierung die Beteiligung von Unternehmen wie Huawei und ZTE am Mobilfunksektor auf die Sicherheit und die Integrität der Kommunikationsinfrastruktur in Hessen?
- Frage 2 Mit welchen Sicherheitsrisiken ist im Zusammenhang mit der Verwendung von Huawei-Technologie im Mobilfunksektor zu rechnen?
- Frage 9 Befürwortet die Landesregierung den Verzicht von Mobilfunktechnologie (z. B. Komponenten von Huawei) aus China?

Die Fragen 1, 2 sowie 9 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Landesregierung befürwortet Bemühungen zur Stärkung der Sicherheit der Mobilfunknetze und einen strikten Umgang mit aufgedeckten Sicherheitsrisiken. Vermieden werden sollte, dass sich die Mobilfunkversorgung aufgrund eines Verbots von Bauteilen drastisch verschlechtert oder gefährdet wird. Die Regelungskompetenz für den Mobilfunksektor und die Kommunikationsinfrastruktur liegt beim Bund. Das Telekommunikationsgesetz des Bundes (TKG) hat den Zweck, durch technologie neutrale Regulierung den Wettbewerb im Bereich der Telekommunikation und leistungsfähige Telekommunikationsinfrastrukturen zu fördern und flächendeckend angemessene und ausreichende Dienstleistungen zu gewährleisten (§ 1 TKG).

Die Landesregierung unterstützt den europäischen „Open RAN“-Ansatz (Open Radio Access Network) der O-RAN Alliance, der sicherstellen soll, dass Hard- und Software von unterschiedlichen Lieferanten grundsätzlich kompatibel sind und die Abhängigkeit von großen Herstellern reduziert wird.

- Frage 3 Wie kann die Landesregierung sicherstellen, dass Cybersicherheitsstandards und Datenschutzrichtlinien eingehalten werden, insbesondere in Bezug auf potenzielle Bedrohungen aus Ländern wie China und Russland?

Die Landesregierung stellt durch die Umsetzung und Anwendung des Hessischen Gesetzes zum Schutz der elektronischen Verwaltung (HITSiG) sowie der Informationssicherheitsleitlinie (ISLL) die Einhaltung der Cybersicherheitsstandards und Datenschutzrichtlinien sicher.

- Frage 4 Welche Maßnahmen ergreift die Landesregierung, um das Risiko von Cybersicherheitsbedrohungen zu minimieren und die Resilienz gegenüber Angriffen zu stärken?
- Frage 5 Inwiefern könnten nach Ansicht der Landesregierung geopolitische Spannungen zwischen China, Russland und dem Westen die Cybersicherheit beeinträchtigen?

Frage 6 Welche Vorkehrungen werden getroffen, um dieser Herausforderung rechtzeitig zu begegnen?

Die Zuordnung des Angreifers zu einem Staat ist bei Cyberattacken teilweise nicht möglich, da die Angriffe im Verborgenen stattfinden. Die Bedrohungslage im Bereich der Cyber- und Informationssicherheit ist hoch. Seit dem Beginn des russischen Angriffs auf die Ukraine am 24.02.2022 konnten deutschlandweit vermehrt Hackingangriffe auf staatsnahe und unternehmerische Infrastrukturen festgestellt werden.

Die Landesregierung verfolgt deshalb unterschiedliche Ansätze, um Cybersicherheitsrisiken zu minimieren und die Resilienz gegen derartige Angriffe zu stärken. Dazu gehören u.a.:

- Das Aufgabenspektrum des CyberCompetenceCenter (Hessen3C) erstreckt sich vom Schutz der Landesverwaltung vor Cybersicherheitsbedrohungen über die Unterstützung der Sicherheitsbehörden bei der Ausbildung von Experten, der Bekämpfung von Cybercrime und Cyberspionage, bis hin zur Beratung von Kommunen, Unternehmen und Betreibern Kritischer Infrastrukturen (KRITIS).
- Das Land nahm auch an der neunten Länder- und Ressortübergreifenden Krisenmanagementübung teil, um die Krisenstrukturen des Landes im Rahmen der Stabsrahmenübung LÜKEX 2023 „Cyberangriff auf das Regierungshandeln“ zu prüfen.
- Mit Angeboten von Schulungen und Präventionsmaßnahmen zum Thema Cybersicherheit werden sowohl die Landesverwaltung als auch Kommunen gestärkt.
- Der von der Landesregierung benannte Informationssicherheitsbeauftragte der hessischen Landesverwaltung (CISO) hat den übergeordneten Auftrag die Informationssicherheit in der Landesverwaltung zu verbessern sowie die Staatskanzlei und Ressorts zu beraten. Er vertritt die hessische Landesverwaltung in Belangen der Informationssicherheit nach außen.
- Mit dem Hessischen Gesetz zum Schutz der elektronischen Verwaltung (HITSiG) wurde die rechtliche Grundlage zur Steigerung der Sicherheit in der Informationstechnik im Land geschaffen.

Frage 7 Welche Rolle spielen nach Ansicht der Landesregierung die Regulierungsbehörden bei der Gewährleistung der Cybersicherheit in Bezug auf die Nutzung von Huawei-Technologie und anderer Hersteller?

Frage 8 Welche Anstrengungen unternimmt Hessen, um die Transparenz und Überprüfbarkeit von Mobilfunkinfrastruktur zu verbessern und potenzielle Sicherheitslücken zu identifizieren?

Die Fragen 7 und 8 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Regulierungsbehörden sind an die geltende Rechtslage in Bund und Ländern gebunden und setzen diese durch.

Das Telekommunikationsgesetz verpflichtet alle Betreiber von TK-Netzen in Deutschland ein Sicherheitskonzept zu erarbeiten und dieses mit der Bundesnetzagentur abzustimmen; der „Sicherheitskatalog 2.0“ regelt, welche Maßnahmen von diesem Konzept erfasst werden müssen. Auch die Einhaltung des Sicherheitskonzepts wird durch die Bundesnetzagentur und externe Audits überwacht. Sämtliche Bauteile aller Hersteller müssen der Sicherheitsprüfung unterzogen werden. Aufgrund der Lage nach Beginn des Ukrainekrieges im Februar 2022 wurde die Bundesnetzagentur vom Bundesministerium für Digitales und Verkehr (BMDV) gebeten, ein regelmäßiges Berichtswesen einzurichten, das insbesondere den Sachstand zur Sicherheit der Telekommunikationsnetze und Telekommunikationsdienste sowie zur Sicherstellung der Versorgung mit Telekommunikationsdiensten erfasst. Das Berichtswesen umfasst auch Sicherheitsvorfälle mit beträchtlichen Auswirkungen auf den Betrieb der Telekommunikationsnetze. In dieses Berichtswesen ist Hessen eingebunden und partizipiert an der allgemeinen Lagebeobachtung.

Wiesbaden, 23. März 2024

Prof. Dr. Roman Poseck