



HESSISCHER LANDTAG

30. 09. 2024

Kleine Anfrage

Markus Fuchs (AfD), Karsten Bletzer (AfD) und Christian Rohde (AfD)
vom 26.06.2024

Einsatz chinesischer IT-Produkte in der Verwaltung

und

Antwort

Ministerin für Digitalisierung und Innovation

Vorbemerkung Fragesteller:

Nach Auskunft der Hessischen Zentrale für Datenverarbeitung (HZD) sind fast 86.000 IT-Arbeitsplätze mit dem HessenPC ausgestattet. Ein Großteil der Geräte stammt von Fujitsu und ist mit dem Label „Made in Japan“ versehen. Bereits im Jahr 2023 hat Fujitsu allerdings bekannt gegeben, den Verkauf von Laptops und Desktop-PCs zum April 2024 in Europa einzustellen. Künftig sollen Geräte der Firma Lenovo für den HessenPC eingesetzt werden, welche über die Firma Bechtle bezogen werden. Lenovo ist allerdings ein chinesisches Unternehmen und geriet in den Jahren 2022 und 2023 wegen schwerer Sicherheitslücken bei seinen Notebook-Modellen in die Schlagzeilen der IT-Presse.

Die Vorbemerkung der Fragesteller vorangestellt, beantworte ich die Kleine Anfrage im Einvernehmen mit dem Minister des Innern, für Sicherheit und Heimatschutz wie folgt:

Frage 1 In welchem Umfang sollen künftig Geräte der Firma Lenovo für den HessenPC verwendet werden? Bitte die Anzahl der minimal und maximal zu erwartenden Anschaffungen aufgeschlüsselt nach Geräteart (Laptop, Desktop, et cetera).

Die Beschaffung der Hardware obliegt der Hessischen Zentrale für Datenverarbeitung (HZD), welche in der Regel einen Rahmenvertragspartner beauftragt. Die HZD hat dabei keinen Einfluss auf den Hersteller der Geräte, die vom Rahmenvertragspartner geliefert werden. Eine Vorgabe eines bestimmten Herstellers ist vergaberechtlich unzulässig.

Frage 2 Gab es Angebote mit Geräten anderer Hersteller beziehungsweise wurden solche eingeholt? Bitte die Antwort begründen.

Frage 3 Wie wurde die Entscheidung zugunsten der Geräte der Firma Lenovo getroffen? Bitte die Antwort begründen und angeben, warum nicht Geräte eines anderen Herstellers (zum Beispiel) genommen wurden.

Die Fragen 2 und 3 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Der Gerätebeschaffung liegt ein europaweites Ausschreibungsverfahren zu Grunde. Dabei wird die Hardware produktneutral unter Angabe der benötigten beziehungsweise gewünschten Leistungsmerkmale ausgeschrieben. Der Zuschlag erfolgt auf Basis der Kriterien Preis / Leistung. Im Rahmen des zuletzt durchgeführten Vergabeverfahrens wurden Geräte des Herstellers Lenovo angeboten (Volumen- / Standardmodelle), einzig für Sondermodelle wurden Geräte der Hersteller Dell oder Panasonic angeboten.

Frage 4 Hält die HZD Rücksprache mit der Landesregierung, bevor Entscheidungen zugunsten bestimmter Hersteller getroffen werden? Antwort bitte begründen.

Frage 5 Gibt die Landesregierung der HZD bestimmte Hersteller von Hardware als vorzugswürdig vor? Antwort bitte begründen.

Die Fragen 4 und 5 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Die Landesregierung gibt keine bestimmten Hersteller von Hardware vor, da aufgrund der ver-
gaberechtlichen Rahmenbedingungen eine herstellernerneutrale Ausschreibung erfolgen muss.

Frage 6 Wurde der Auftrag der HZD über die Vergabeplattform Hessen ausgeschrieben? Antwort bitte
begründen.

Das Vergabeverfahren wurde auf der Vergabeplattform Hessen ausgeschrieben. Die Veröffent-
lichung erfolgte darüber hinaus auf der Ausschreibungsplattform der Europäischen Union (TED)
und der Hessischen Ausschreibungsdatenbank (HAD).

Frage 7 Sieht die Landesregierungen – angesichts der zunehmenden politischen und militärischen
Spannungen zwischen der Volksrepublik China und den USA – möglich Probleme in der Hard-
wareabhängigkeit des Landes Hessen von einem chinesischen Hersteller? Antwort bitte begründen.

Bei den Ausschreibungen für Soft- und Hardware erhalten regelmäßig Anbieter aus Europa und
den USA den Zuschlag, was dem Entstehen von eventuellen Abhängigkeiten zu autoritären
Staaten entgegensteht. Sofern vereinzelt chinesische Produkte eingesetzt werden, begründet die
Nutzung alleine noch keine Abhängigkeit.

Grundsätzlich besteht immer ein Risiko, dass Hersteller wissentlich oder unwissentlich Schwach-
stellen in ihren Produkten verbauen. Das konkrete Risiko der eingesetzten Hardware wird bei der
Erstellung der IT-Sicherheitskonzepte gemäß dem IT-Grundschutz nach dem Bundesamt für
Sicherheit in der Informationstechnik geprüft und bewertet.

Im Rahmen dieser Überprüfung wird vom Fachverfahrensverantwortlichen entschieden, ob und
wie die durch das mehrschichtige Sicherheitssystem im Netzbereich relativierten Risiken weiter
kompensiert werden können.

Frage 8 Welche konkreten Maßnahmen hat die Landesregierung ergriffen, um den Einsatz von Hardware
und Software aus Diktaturen zu vermindern? Antwort bitte begründen.

Exemplarisch lässt sich, mit Blick auf den russischen Angriffskrieg gegen die Ukraine, konstatie-
ren, dass es auf allen relevanten Ebenen Bestrebungen gibt, den Einsatz von Hard- und Software
aus Diktaturen signifikant zu reduzieren. So wurde etwa das seit der völkerrechtswidrigen
Annexion der Krim gegenüber Russland bestehende Sanktionsregime (Verordnung (EU)
Nr. 833/2014) entsprechend angepasst und erweitert. Es umfasst nunmehr auch Sanktionen, die
die Vergabe und Ausführung öffentlicher Aufträge und Konzessionen ab Erreichen der EU-
Schwellenwerte nach § 106 des Gesetzes gegen Wettbewerbsbeschränkungen unmittelbar be-
treffen. Konkret gilt für noch nicht abgeschlossene Vergabeverfahren seit dem 09.04.2022 ein
Zuschlagsverbot. Gleichzeitig wurde, für bereits vor dem 09.04.2022 vergebene Aufträge und
Konzessionen, ab dem 11.10.2022 ein Vertragserfüllungsverbot verhängt (Artikel 5 k der Ver-
ordnung (EU) 2022/576 des Rates vom 08.04.2022 zur Änderung der Verordnung (EU)
Nr. 833/2014).

Frage 9 Welche konkrete Maßnahme wurden ergriffen, um zu verhindern, dass in den HessenPC Bestand-
teile (Hardware oder Software) verwendet werden, welche einen Zugriff feindlicher Nachrichten-
dienste zum Zwecke der Sabotage ermöglichen? Antwort bitte begründen.

Im Technischen Release- und Entwicklungszentrum der HZD findet eine intensive, kontinuier-
liche Prüfung der Windows Major Releases statt. Betrachtet und dokumentiert werden neue Funk-
tionalitäten, Änderungen und unerwünschter Datenabfluss des Betriebssystems. Erst auf Basis
dieser Vorarbeiten entsteht jedes neue, auf die Bedürfnisse der Landesverwaltung zugeschnittene
Major Release des HessenPC.

Im Aufgabenbereich des Zentralen Virenschutzes der HZD werden außerdem geeignete Maß-
nahmen ergriffen, um einen Schutz vor Cyberangriffen proaktiv zu gewährleisten und Angriffe
abzuwehren. Hierzu gehören:

- ENS/ENSL (Klassischer Virenschutz): Überprüft Dateien und Prozesse mittels Virenerken-
nungen, die auf Pattern und Heuristik basieren, sobald diese in Bearbeitung genommen
werden. Über eine weltweite Datenbank (GTI) des Herstellers werden neue Erkennungen in
Echtzeit aktualisiert.
- Zugriffsschutz: Unterbindet Zugriffe auf Windows-Betriebssystem-Ordner, die bei Außen-
angriffen zur Einschleusung von Erpressungssoftware verwendet werden.

- ATP (Adaptive Threat Protection) zur Abwehr von bisher unbekanntem Malicious Code: Überwacht Prozesse und Prozessketten auf Basis ihres Verhaltens und isoliert Prozesse bei Auffälligkeiten. Es findet eine automatisierte Analyse in einer Sandboxumgebung statt. Prozesse können nur noch in einer virtualisierten Umgebung gestartet werden.
- TIE (Reputationsdatenbank): Ausführbare Dateien werden auf Basis eines Regelwerks und der weltweiten Datenbank (GTI) des Herstellers in ihrer Reputation bewertet und entsprechende Aktionen abgeleitet.
- TSME (Trellix Security for Microsoft Exchange): Schutz der zentralen E-Mail-Plattform. Die Anwendung ist im Verbund des Virenschutzes implementiert und nutzt die Komponenten TIE und Sandbox.
- TSMS (Trellix Security for Microsoft Sharepoint): Schutz der externen Sharepoint Server. Die Anwendung ist im Verbund des Virenschutzes implementiert und nutzt die Komponenten TIE und Sandbox.
- Cava Schnittstelle: Schutz der Dateiablagen (Storage).

Frage 10 Ist Hessen vom chinesischen i-Soon-Hackerangriff betroffen? Antwort bitte begründen.

Der Landesregierung liegen keine Erkenntnisse oder Meldungen vor, die die Annahme rechtfertigen, dass hessische Dienststellen vom genannten Vorfall betroffen sind.

Eine Prüfung des Datenverkehrs zwischen bekannten Infrastrukturen der Angreifer und dem Netz der Hessischen Landesregierung hat ebenfalls keine Betroffenheit aufgezeigt.

Wiesbaden, 16. September 2024

Prof. Dr. Kristina Sinemus