



HESSISCHER LANDTAG

30. 01. 2025

Kleine Anfrage

Markus Fuchs (AfD), Karsten Bletzer (AfD) und Christian Rohde (AfD)
vom 15.10.2024

Softwarezertifizierung und digitale Resilienz

und

Antwort

Minister des Innern, für Sicherheit und Heimatschutz

Vorbemerkung Fragesteller:

Die Anzahl der Cyber-Angriffe und Softwarepannen nimmt exponentiell zu. Zuletzt führte ein fehlerhaftes Update der Cybersicherheitsfirma CrowdStrike zu weltweiten Ausfällen von mit Microsoft Windows ausgestatteten Computersystemen. Das Uniklinikum Schleswig-Holstein beabsichtigt laut Presse diesbezüglich inzwischen Schadensersatz einzufordern. Ein Problem dabei ist, dass die Firma CrowdStrike laut Presse den Einsatz ihres Falcon-EDR-Sensors in kritischen Infrastrukturen (KRITIS) gerade nicht empfiehlt. Laut verschiedener Experten ist ein Haftungsdurchgriff auf den – in der Regel im außereuropäischen Ausland ansässigen Hersteller – gegenwärtig praktisch kaum möglich und für den Normalbürger sicherlich keinesfalls realisierbar. Weiterhin wird festgestellt, dass es keine gesetzlich normierten allgemeinen Mindestqualitätsstandards für Software gibt, auch fehlt es weitgehend an aussagekräftigen Zertifikaten, welche den Käufern eine Beurteilung von Software ermöglichen. Einer Zulassung durch das BSI bedürfen lediglich Produkte im Sinne der §§ 51, 52 VSA. Für Kraftfahrzeuge und Flugzeuge ist die Situation anders. Kein Fahrzeug oder Flugzeug darf in Deutschland zum Beispiel fahren oder fliegen, ohne dass es eine entsprechende Typengenehmigung beziehungsweise Verkehrszulassung durch das Kraftfahrt-Bundesamt oder das Luftfahrt-Bundesamt erhalten hat. Auch für Pharmazeutika und Lebensmittel gibt es Regeln, die analog für Software fehlen. Dies wird in der Wissenschaft und auch von Datenschützern stark kritisiert.

Die Vorbemerkung der Fragesteller vorangestellt, beantworte ich die Kleine Anfrage im Einvernehmen mit dem Chef der Staatskanzlei, mit dem Minister für Bundes- und Europaangelegenheiten, Internationales und Entbürokratisierung und Bevollmächtigten des Landes Hessen beim Bund, dem Minister der Finanzen, dem Minister der Justiz und für den Rechtsstaat, dem Minister für Kultus, Bildung und Chancen, dem Minister für Wissenschaft und Forschung, Kunst und Kultur, dem Minister für Wirtschaft, Energie, Verkehr, Wohnen und ländlichen Raum, der Ministerin für Digitalisierung und Innovation, dem Minister für Landwirtschaft und Umwelt, Weinbau, Forsten, Jagd und Heimat, der Ministerin für Familie, Senioren, Sport, Gesundheit und Pflege und der Ministerin für Arbeit, Integration, Jugend und Soziales wie folgt:

- Frage 1 Welche Notfall-Szenarien werden durch die für die Cybersicherheit der KRITIS Verantwortlichen in Hessen geübt? Die Antwort bitte begründen und dabei nach Szenario, der Übungsart (im Sinne von BSI-Standard 100-4 [Version 1 (2004) S. 85 Tabelle 18.]), der Anzahl der Übungen pro Zeiteinheit und der übenden Stelle differenzieren.
- Frage 2 Ist bei den gegebenen Systemen der KRITIS überprüft worden, dass innerhalb der vorgesehenen Ausfallzeit auf das Notfallsystem umgeschaltet wird? Die Antwort bitte begründen.

Die Fragen 1 und 2 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Für die Cybersicherheit in KRITIS sind die Betreiber der KRITIS verantwortlich. Von staatlicher Seite übt das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Bereich Cybersicherheit die Aufsicht aus.

- Frage 3 Beabsichtigt die Landesregierung sich auf der Ebene des Bundes und der EU für eine Verbesserung der rechtlichen Situation von Softwarekäufern und Software-Pannenbetroffenen einzusetzen? Die Antwort bitte unter Erläuterung möglicher Maßnahmen begründen.

Der Europäische Rat hat im Oktober 2024 eine Neufassung der Produkthaftungsrichtlinie 85/374/EWG beschlossen. Diese sieht unter anderem eine Ausweitung der Rechte von Betroffenen bei fehlerhaften Softwareprodukten vor. Die Mitgliedstaaten sind verpflichtet, diese

Richtlinie in nationales Recht umzusetzen. Die Zuständigkeit liegt beim Bund. Es gibt keine Anhaltspunkte dafür, dass der Bund die Richtlinie nicht fristgerecht umsetzt.

Frage 4 a) Beabsichtigt die Landesregierung sich für die Schaffung von Softwarequalitätszertifikaten einzusetzen? Die Antwort bitte begründen.

Frage 4 b) Auf welche Auffassungen in der Wissenschaft stützt die Landesregierung ihre Position in Bezug auf die Frage 4 a)? Die Antwort bitte begründen.

Die Fragen 4 a) und 4 b) werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Für Produkte der Informationstechnik bestehen international anerkannte Sicherheitszertifikate (beispielsweise auf Basis von Information Technology Security Evaluation Criteria, Common Criteria oder nach Technischen Richtlinien).

Frage 4 c) Inwiefern teilt die Landesregierung die von der Leiterin des Lehrstuhls „Sicherheit in der Informatik“ an der School of Computation, Information and Technology der Technischen Universität München sowie Leiterin des Fraunhofer-Instituts für Angewandte und Integrierte Sicherheit (AISEC) in Garching bei München in ihrem Vortrag zur IT-Sicherheit – im Rahmen einer Veranstaltung des Deutschen Museum München und der Deutschen Akademie der Technikwissenschaften – am 28.09.2022 vorgenommenen Einschätzungen zur Rolle der Politik im Bereich der IT-Sicherheit? Die Antwort bitte in Bezug auf die dort genannten Einzelpunkte begründen.

Der Landesregierung erschließt sich nicht, auf welche Passage des 90-minütigen Vortrags sich die Frage bezieht.

Frage 5 Beabsichtigt die Landesregierung die Vergaberichtlinien für öffentliche Aufträge im Bereich von Software und Hardware so anzupassen, dass künftig nur hinsichtlich der Sicherheit zertifizierte Produkte beschafft werden dürfen? Die Antwort bitte begründen.

Das Vergaberecht bietet bereits die Möglichkeit, Beschaffungen von der Erfüllung bestimmter Sicherheitsanforderungen abhängig zu machen.

Frage 6 Gibt es bestimmte (staatliche) Bereiche (insbesondere in der KRITIS) in denen aus Sicherheitsgründen von einer Digitalisierung oder Vernetzung abgesehen werden sollte? Die Antwort bitte unter Angabe der Bereiche und der jeweils für die Beurteilung der Sicherheitsgründe verwendeten Kriterien, Metriken et cetera begründen.

Bei der Digitalisierung von Geschäftsprozessen und Verwaltungsaufgaben ist ein Sicherheitskonzept zu erstellen. Sofern in diesem Zusammenhang kritische Risiken identifiziert werden, für die keine angemessenen Schutzmaßnahmen umgesetzt werden können, wird von einer Digitalisierung abgesehen. Dies sichert einen verantwortungsvollen Umgang mit Sicherheitsrisiken im Bereich der Soft- und Hardware-Produkte und IT-Lösungen.

Frage 7 Welche Prüfverfahren werden angewendet, um das Vorhandensein von „Hintertüren“ in der durch das Land Hessen oder die KRITIS genutzten Hard- und Software auszuschließen? Die Antwort bitte unter Benennung und Schilderung der Verfahren begründen.

Das Hessische Gesetz zum Schutz der elektronischen Verwaltung (HITSiG) und die Informationssicherheitsleitlinie der hessischen Landesverwaltung geben Rahmen, Ziele und Grundsätze der Informationssicherheit vor. Sie legen die zu schützenden Grundwerte (Vertraulichkeit, Integrität, Verfügbarkeit) als auch Maßnahmen und Prozesse fest. In Bezug auf die Prüfverfahren sind durch die Vorgabe der Einführung eines Informationssicherheitsmanagement Systems (ISMS) in den Dienststellen zahlreiche spezifische Prüfverfahren im Rahmen des kontinuierlichen Verbesserungsprozesses des ISMS etabliert. Hiernach sind für alle IT-Systeme und -Verfahren Informationssicherheitskonzepte einschließlich einer Schutzbedarfsfeststellung zu erstellen. Die Sicherheitskonzepte haben den BSI-Standards (BSI 200-1, BSI 200-2 und BSI 200-4) zu entsprechen.

Frage 8 In welchem Umfang setzt das Land Hessen Produkte im Sinne der §§ 51, 52 VSA ein, die eine BSI-Zulassung haben? In der Antwort bitte die Anzahl, die Art des Produkts und den Einsatzzweck angeben.

Die Landesverwaltung setzt insgesamt vier Hard- und Softwareprodukte zur Verschlüsselung von Daten bei der Telekommunikation ein.