Landtag von Baden-Württemberg **Drucksache 18 / 547**
18. Wahlperiode **24.9.2026**

Kleine Anfrage

des Abg. Daniel Lindenschmid AfD

und

Antwort

des Ministeriums des Inneren, für Digitalisierung und Europa

Resilienz der Landes-IT gegenüber fehlerhaften Softwareupdates und Herstellerabhängigkeiten

Kleine Anfrage

Ich frage die Landesregierung:

1. Welche Behörden, Einrichtungen oder Beteiligungen des Landes waren nach Kenntnis der Landesregierung von dem nach medialer Berichterstattung fehlerhaften Crowd Strike-Softwareupdate vom 19. Juli 2024 unmittelbar oder mittelbar betroffen?

2. Welche Verwaltungsleistungen oder sonstigen Dienste waren dadurch in welchem Zeitraum eingeschränkt (z. B. nicht verfügbar)?

3. Welche unmittelbaren Kosten und sonstigen quantifizierbaren Schäden sind dem Land infolge des Vorfalls entstanden?

4. Welche vertraglichen Ansprüche auf Ersatz, Gutschrift oder sonstigen Ausgleich wurden geprüft oder geltend gemacht mit der Bitte um Angabe des Ergebnisses?

5. Welche organisatorischen und technischen Änderungen hat die Landesregierung seit dem Vorfall vorgenommen, um fehlerhafte oder kompromittierte Softwareupdates vor einer breiten Ausbringung zu erkennen und ihre Folgen zu begrenzen?

6. In welchen Bereichen der Landesverwaltung bestehen Verfahren mit gestuften Test- und Freigaberingen, Rückfallmöglichkeiten sowie offline verfügbaren Wiederanlauf- und Wiederherstellungsplänen?

7. Inwieweit wurden die Wiederanlauf- und Wiederherstellungsverfahren für kritische IT-Dienste seit dem 1. Januar 2024 praktisch getestet, mit Darlegung der wesentlichen Defizite, die dabei festgestellt wurden?

8. Nach welchen Kriterien bewertet die Landesregierung Konzentrations-, Lieferketten- und Ausfallrisiken bei der Beschaffung zentraler Hard- und Software sowie von Cloud- und Sicherheitsdiensten?

Eingegangen: 24.9.2026 / Ausgegeben: 20.10.2026

Drucksachen und Plenarprotokolle sind im Internet abrufbar unter: www.landtag-bw.de/Dokumente

Der Landtag druckt auf Recyclingpapier, ausgezeichnet mit dem Umweltzeichen „Der Blaue Engel“.

9. Für welche besonders kritischen Produkt- oder Dienstkategorien bestehen Exit-, Migrations- oder Ersatzstrategien, wenn ein Anbieter oder Produkt kurzfristig ausfällt oder nicht mehr eingesetzt werden kann?

10. Welche konkreten Maßnahmen hat das Land seit Juli 2024 ergriffen, um digitale Souveränität, Interoperabilität und den Einsatz offener Standards sowie geeigneter Open-Source-Lösungen zu stärken (bitte einschließlich verausgabter Mittel und erreichter Meilensteine darstellen)?

15.9.2026

Lindenschmid AfD

Begründung

Der IT-Ausfall vom 19. Juli 2024 stand im Zusammenhang mit einem fehlerhaften CrowdStrike-Update. Nach Angaben des Herstellers war der Vorfall nicht auf einen Cyberangriff zurückzuführen. Die Kleine Anfrage soll vor diesem Hintergrund klären, welche Folgen der Vorfall für das Land hatte und welche Vorkehrungen für Test, Rückfall, Wiederanlauf und Anbieterwechsel bestehen.

Antwort

Mit Schreiben vom 15. Oktober 2026 Nr. IM5-0141.5-806/1/2 beantwortet das Ministerium des Inneren, für Digitalisierung und Europa die Kleine Anfrage wie folgt:

1. Welche Behörden, Einrichtungen oder Beteiligungen des Landes waren nach Kenntnis der Landesregierung von dem nach medialer Berichterstattung fehlerhaften CrowdStrike-Softwareupdate vom 19. Juli 2024 unmittelbar oder mittelbar betroffen?

2. Welche Verwaltungsleistungen oder sonstigen Dienste waren dadurch in welchem Zeitraum eingeschränkt (z. B. nicht verfügbar)?

3. Welche unmittelbaren Kosten und sonstigen quantifizierbaren Schäden sind dem Land infolge des Vorfalls entstanden?

4. Welche vertraglichen Ansprüche auf Ersatz, Gutschrift oder sonstigen Ausgleich wurden geprüft oder geltend gemacht mit der Bitte um Angabe des Ergebnisses?

Die Fragen 1 bis 4 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Nach Kenntnis der Landesregierung setzte die Landesverwaltung zum Zeitpunkt des Vorfalls keine Produkte des Herstellers CrowdStrike ein und setzt solche Produkte auch gegenwärtig nicht ein. Entsprechend waren Behörden und Einrichtungen des Landes von dem fehlerhaften CrowdStrike-Softwareupdate vom 19. Juli 2024 nicht betroffen. Zu einer Betroffenheit von Beteiligungen des Landes liegen der Landesregierung keine Erkenntnisse vor. Einschränkungen von Verwaltungsleistungen oder sonstigen Diensten sowie hieraus resultierende Kosten oder sonstige quantifizierbare Schäden sind nicht bekannt geworden. Mangels Betroffenheit bestand auch kein Anlass, vertragliche Ansprüche auf Ersatz, Gutschrift oder sonstigen Ausgleich geltend zu machen.

5. Welche organisatorischen und technischen Änderungen hat die Landesregierung seit dem Vorfall vorgenommen, um fehlerhafte oder kompromittierte Softwareupdates vor einer breiten Ausbringung zu erkennen und ihre Folgen zu begrenzen?

6. In welchen Bereichen der Landesverwaltung bestehen Verfahren mit gestuften Test- und Freigaberingen, Rückfallmöglichkeiten sowie offline verfügbaren Wiederanlauf- und Wiederherstellungsplänen?

Die Fragen 5 und 6 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

In der Landesverwaltung bestehen etablierte Verfahren, um Risiken im Zusammenhang mit der Einführung und Aktualisierung von Software zu begrenzen.

Im Zuständigkeitsbereich des IT-Dienstleisters des Landes, der BITBW, erfolgt die Ausbringung von Softwareupdates im Rahmen eines geregelten Change-Management-Prozesses. Dieser umfasst einen expliziten Test- und Freigabeprozess und beinhaltet auch Regelungen für einen Rollback, also das Zurücksetzen auf den vorherigen Stand.

Auch in der Finanzverwaltung werden neue Softwareprodukte vor ihrem Einsatz in der Produktionsumgebung in einer Test- und Referenzumgebung erprobt und auf Fehler untersucht. Zusätzlich erfolgen grundsätzlich Schwachstellenscans und erforderlichenfalls Penetrationstests. Werden hierbei Fehler oder Schwachstellen erkannt, erfolgt kein Einsatz in der Produktionsumgebung.

7. Inwieweit wurden die Wiederanlauf- und Wiederherstellungsverfahren für kritische IT-Dienste seit dem 1. Januar 2024 praktisch getestet, mit Darlegung der wesentlichen Defizite, die dabei festgestellt wurden?

Die BITBW verfügt über einen mehrjährigen Plan für Notfallübungen, der fortlaufend umgesetzt wird. Die hierbei gewonnenen Erkenntnisse werden im Rahmen eines Lessons-Learned-Prozesses aufgearbeitet und entsprechende Folgemaßnahmen umgesetzt.

Auch in der Finanzverwaltung werden Wiederanlauf- und Wiederherstellungsverfahren regelmäßig praktisch erprobt. Im Frühjahr 2026 wurde eine Umschaltung auf das Notfallrechenzentrum mit anschließender Rückumstellung auf das Hauptrechenzentrum erfolgreich durchgeführt. Im September 2026 fand zudem eine länderübergreifende Notfallübung im Rahmen des bundesweiten Vorhabens KONSENS statt.

8. Nach welchen Kriterien bewertet die Landesregierung Konzentrations-, Lieferketten- und Ausfallrisiken bei der Beschaffung zentraler Hard- und Software sowie von Cloud- und Sicherheitsdiensten?

Bei der Beschaffung zentraler Hard- und Software sowie von Cloud- und Sicherheitsdiensten werden Anforderungen der Informationssicherheit und des Risikomanagements berücksichtigt. Die BITBW verfügt hierzu über einen am BSI-IT-Grundschutz ausgerichteten Beschaffungsprozess mit standardisierten Anforderungen an die Informationssicherheit. Ergänzend besteht ein Risikomanagement zur Bewertung und Steuerung von Dienstleistern, mit dem insbesondere Konzentrations-, Lieferketten- und Ausfallrisiken möglichst gering gehalten werden sollen.

9. Für welche besonders kritischen Produkt- oder Dienstkategorien bestehen Exit-, Migrations- oder Ersatzstrategien, wenn ein Anbieter oder Produkt kurzfristig ausfällt oder nicht mehr eingesetzt werden kann?

Für zahlreiche kritische Produkte und Leistungen im Zuständigkeitsbereich der BITBW bestehen sogenannte Dual-Vendor-Konzepte. Von einer näheren Darstellung der betroffenen Produkt- und Dienstkategorien sowie weitergehender Informationen wird aus Sicherheitsgründen abgesehen.

10. Welche konkreten Maßnahmen hat das Land seit Juli 2024 ergriffen, um digitale Souveränität, Interoperabilität und den Einsatz offener Standards sowie geeigneter Open-Source-Lösungen zu stärken (bitte einschließlich verausgabter Mittel und erreichter Meilensteine darstellen)?

Die Stärkung der digitalen Souveränität, der Interoperabilität sowie die Berücksichtigung offener Standards und geeigneter Open-Source-Lösungen sind Daueraufgaben bei der Weiterentwicklung der IT der Landesverwaltung. Sie sind in den Vorgaben für die IT der Landesverwaltung verankert. Die BITBW setzt die Vorgaben der VwV IT-Standards unter Berücksichtigung von Kosten und Nutzen um und bevorzugt dabei nach Möglichkeit Open-Source-Lösungen.

Auch in der Steuerverwaltung des Landes werden bereits seit Jahren Open-Source-Lösungen eingesetzt. Im Innendienst kommt ausschließlich das Open-Source-Office-Paket LibreOffice zum Einsatz. Als Betriebssystem der Thin Clients wird das Linuxbasierte Betriebssystem eLux eingesetzt. Auch die weit überwiegende Zahl der virtualisierten Server wird unter Linux betrieben. Im Datenbankbereich werden überwiegend PostgreSQL und MySQL eingesetzt. Proprietäre Datenbanksysteme werden schrittweise durch Open-Source-Lösungen abgelöst.

Hagel

Minister des Inneren,
für Digitalisierung und Europa