Landtag von Baden-Württemberg **Drucksache 17 / 10115**

17. Wahlperiode **8.1.2026**

Antrag

der Abg. Daniel Karrais und
Hans Dieter Scheerer u. a. FDP/DVP

und

Stellungnahme

des Staatsministeriums

Cyberangriff auf den THE LÄND-Onlineshop

Antrag

Der Landtag wolle beschließen,

die Landesregierung zu ersuchen

zu berichten,

1. wie viele Kunden den THE LÄND-Onlineshop seit dessen Start bis heute nutzen;

2. wann sich der Cyberangriff auf den THE LÄND-Onlineshop konkret ereignet hat;

3. inwiefern sie konkrete Informationen zu der von den Angreifern ausgenutzten Sicherheitslücke im Shopsystem hat, insbesondere wie diese Sicherheitslücke entstehen konnte;

4. inwiefern das Risiko besteht, dass es weitere Sicherheitslücken im Shopsystem gibt;

5. wie sowie zu welchem Zeitpunkt der Cyberangriff auf den Onlineshop entdeckt worden ist;

6. welche Schritte sie nach dem Bekanntwerden des Cyberangriffs konkret ergriffen hat;

7. wie sowie zu welchem Zeitpunkt sie die Kunden über den Cyberangriff informiert hat (bitte auch mit Angabe, wie viele Kunden dem Cyberangriff zum Opfer gefallen sind);

8. welche Schäden konkret entstanden sind (bitte differenziert nach Betroffenen und Schaden);

Eingegangen: 8.1.2026 / Ausgegeben: 6.2.2026

9. welche Möglichkeiten betroffene Kunden haben, damit diese nicht auf dem Schaden sitzen bleiben;

10. inwiefern das Risiko besteht, dass durch den Cyberangriff Kundendaten wie E-Mail-Adressen etc. abgegriffen wurden;

11. inwiefern im Vorfeld zu Fragen der Cybersicherheit die Cybersicherheitsagentur konsultiert wurde sowie ggf. warum nicht;

12. welche Rückmeldungen ggf. seitens der Cybersicherheitsagentur erfolgten sowie möglicherweise (nicht) umgesetzt wurden;

13. inwiefern sie neben dem THE LÄND-Onlineshop weitere Onlineshops betreibt (bitte ggf. mit konkreter Darstellung der jeweiligen Onlineshops);

14. wie sie das Risiko für Sicherheitslücken in diesen unter Ziffer 13 dargestellten Onlineshops bewertet;

15. welche Konsequenzen sie aus dem Cyberangriff auf den THE LÄND-Onlineshop zieht.

8.1.2026

Karrais, Scheerer, Goll, Weinmann, Haußmann, Dr. Timm Kern, Bonath, Fischer, Haag, Heitlinger, Dr. Jung, Reith, Dr. Schweickert FDP/DVP

Begründung

Laut Informationen des Staatsministeriums haben sich unbekannte Hacker Zugang zum THE LÄND Onlineshop verschafft. Die Angreifer sollen vom 27. bis 29. Dezember 2025 eine bislang unbekannte Sicherheitslücke im Shopsystem ausgenutzt haben. Die Täter richteten laut Staatsministerium eine gefälschte Bezahlseite ein, um Zahlungen einzuziehen. Dem Cyberangriff sind offenbar eine zweistellige Zahl an Kunden zum Opfer gefallen. Der Antrag soll sich nach dem genauen Ausmaß sowie den Konsequenzen des Cyberangriffs erkundigen.

Stellungnahme

Mit Schreiben vom 2. Februar 2026 Nr. STM23-0222-63/4/2 nimmt das Staatsministerium im Einvernehmen mit dem Ministerium des Inneren, für Digitalisierung und Kommunen zu dem Antrag wie folgt Stellung:

1. wie viele Kunden den THE LÄND-Onlineshop seit dessen Start bis heute nutzen;

Zu 1.:

Im THE LÄND FÄNSHOP waren bis zur Offlinesetzung des Shops rund 184 000 Kundenstammsätze angelegt.

2. wann sich der Cyberangriff auf den THE LÄND-Onlineshop konkret ereignet hat;

3. inwiefern sie konkrete Informationen zu der von den Angreifern ausgenutzten Sicherheitslücke im Shopsystem hat, insbesondere wie diese Sicherheitslücke entstehen konnte;

Zu 2. und 3.:

Die Ziffern 2 und 3 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet. Nach aktuellem Stand der Ermittlungen wurde der Onlineshop von THE LÄND, *shop.thelaend.de*, im Zeitraum vom 27. Dezember 2025 bis 29. Dezember 2025 Ziel eines Cyberangriffs. Nach aktuellem Erkenntnisstand wurde als Angriffsvektor eine bis dato nicht bekannte Sicherheitslücke des Shop-Systems ausgenutzt (sog. Zero-Day-Schwachstelle), wodurch die Angreifer Zugriff auf Kundendaten wie Namen, E-Mail-Adressen und verschlüsselte Passwörter erhalten haben. Zudem wurde eine manipulierte Bezahlseite eingerichtet, über die Kreditkartendaten von Kundinnen und Kunden abgegriffen und Zahlungen eingezogen wurden. Die tatsächlich abgebuchten Beträge lagen dabei deutlich über den im Bestellprozess ausgewiesenen Summen.

Für kostenpflichtige Bestellungen stehen im Onlineshop grundsätzlich die Zahlungsmethoden Vorkasse (Überweisung) und PayPal zur Verfügung. Einige Artikel, wie etwa „Nett-hier“-Sticker, können kostenlos bestellt werden.

4. inwiefern das Risiko besteht, dass es weitere Sicherheitslücken im Shopsystem gibt;

5. wie sowie zu welchem Zeitpunkt der Cyberangriff auf den Onlineshop entdeckt worden ist;

6. welche Schritte sie nach dem Bekanntwerden des Cyberangriffs konkret ergriffen hat;

Zu 4., 5. und 6.:

Die Ziffern 4, 5 und 6 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet. Am Samstag, 27. Dezember 2025, gingen die ersten Nachrichten zu Unstimmigkeiten im Bestellprozess im Kontaktpostfach des Shops ein. Aufgrund des Zeitpunktes blieb dies zunächst unbemerkt. Am Montag, 29. Dezember 2025, informierte ein betroffener Kunde die Cyber-Ersthilfe BW der Cybersicherheitsagentur Baden-Württemberg (CSBW). Experten der CSBW vollzogen unmittelbar den vom Melder beschriebenen Angriffsweg nach und konnten die Manipulation des Webshops bestätigen. Die CSBW informierte umgehend das zuständige Referat im Staatsministerium sowie den Ressort-CISO des Staatsministeriums und bot ihre Unterstützung an. Infolgedessen wurden die behördliche Datenschutzbeauftragte sowie alle inhaltlich berührten Organisationseinheiten des

Staatsministeriums, einschließlich der fachlich berührten Dienstleister informiert. Hierunter fallen auch der Logistikdienstleister des Onlineshops sowie die Agentur, welche für das Community Management auf den sozialen Kanälen beauftragt ist.

Um potenzielle weitere Risiken zu minimieren, wurde der Onlineshop sofort nach Bekanntwerden des Vorfalls am 29. Dezember 2025 vorsorglich offline genommen und bleibt bis zur vollständigen Klärung des Sachverhalts sowie bis zum Vorliegen weiterführender Analyseergebnisse außer Betrieb. Die getroffenen Maßnahmen erfolgten in Abstimmung mit dem Shop-Anbieter. Dieser wurde über den Sicherheitsvorfall am 29. Dezember 2025 informiert.

Der Sicherheitsvorfall wurde dem Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg (LfDI) unmittelbar nach Klärung des Sachverhalts am 30. Dezember 2025 angezeigt. Am selbigen Tag wurde beim Landeskriminalamt Baden-Württemberg über die Zentrale Ansprechstelle Cybercrime (ZAC) für Wirtschaftsunternehmen und Behörden durch das Staatsministerium eine Strafanzeige gestellt. Die CSBW war weiterhin beratend tätig und übernahm im Benehmen mit dem StM die forensischen Analysen. Die CSBW warnte zudem am 2. Januar 2026 die Institutionen der Landes- und Kommunalverwaltung durch eine interne Mitteilung vor dem Einsatz der Shop-Software des involvierten Anbieters.

Das Staatsministerium stand seit Bekanntwerden des Vorfalls in engem Austausch mit allen inhaltlich beteiligten Dienststellen und Dienstleistern und führt regelmäßig Lagebesprechungen durch.

7. wie sowie zu welchem Zeitpunkt sie die Kunden über den Cyberangriff informiert hat (bitte auch mit Angabe, wie viele Kunden dem Cyberangriff zum Opfer gefallen sind);

Zu 7.:

Über den Logistikdienstleister des Onlineshops wurde am 31. Dezember 2025 eine E-Mail an alle rund 184 000 Kundinnen und Kunden des Shops versandt, in welcher diese über den Sicherheitsvorfall beim Onlineshop informiert wurden.

Die Täter könnten die Kreditkartendaten von Kunden erhalten haben, die im Zeitraum zwischen dem 27. Dezember 2025 und 29. Dezember 2025 eine Bestellung im Onlineshop getätigt und ihre Kreditkarteninformationen auf der falschen Bezahlseite eingegeben haben – möglicherweise unabhängig davon, ob die Zahlung dann tatsächlich freigegeben wurde. Diese 220 identifizierten Personen, welche im Angriffszeitraum eine Bestellung im Onlineshop ausgelöst haben und auf die manipulierte Bezahlseite umgeleitet wurden, wurden hierüber am 31. Dezember 2025 in einer zusätzlichen E-Mail informiert und gebeten, verdächtige Abbuchungen, insbesondere an das Bankinstitut „Monobank“ zu überprüfen.

Ebenso wurde am 31. Dezember 2025 auf der Shop-Website *(shop.thelaend.de)* die Meldung eingerichtet, dass der Onlineshop aufgrund eines Angriffs auf die technische Infrastruktur vorübergehend nicht erreichbar ist.

Die Pressestelle des Staatsministeriums hat am 31. Dezember 2025 die Öffentlichkeit informiert. Die darauf folgende dpa-Meldung zum Cyberangriff wurde von regionalen und nationalen Medien aufgegriffen.

Anfragen zum Cyberangriff, die im Kontaktpostfach eintreffen, werden seit dem 30. Dezember 2025 kontinuierlich beantwortet.

8. welche Schäden konkret entstanden sind (bitte differenziert nach Betroffenen und Schaden);

10. inwiefern das Risiko besteht, dass durch den Cyberangriff Kundendaten wie E-Mail-Adressen etc. abgegriffen wurden;

Zu 8. und 10.:

Die Ziffern 8 und 10 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet. Nach derzeitigem Erkenntnisstand könnten die Täter durch den Cyberangriff Zugriff auf Daten aller 184 000 Kunden des Onlineshops erhalten haben, darunter auch E-Mail-Adressen.

Die Täter könnten zusätzlich die Kreditkartendaten von 220 Kunden erhalten haben, die im Zeitraum zwischen dem 27. Dezember 2025 und 29. Dezember 2025 eine Bestellung im Onlineshop getätigt und ihre Kreditkarteninformationen auf der manipulierten Bezahlseite eingegeben haben. Im Shop-System selbst werden keine Zahlungsdaten vorgehalten, d. h. an diese konnte der Angreifer nur über die manipulierte Bezahlseite kommen.

Durch Rückmeldungen von Kundinnen und Kunden wird aktuell von einer einstelligen Zahl von finanziell geschädigten Personen ausgegangen, bei welchen unterschiedliche dreistellige Beträge abgebucht wurden.

9. welche Möglichkeiten betroffene Kunden haben, damit diese nicht auf dem Schaden sitzen bleiben;

Zu 9.:

Den Kundinnen und Kunden, bei welchen nach Eingabe ihrer Kreditkartendaten über die manipulierte Bezahlseite ein Geldbetrag abgebucht wurde, wurde vom Landesmarketing eine finanzielle Erstattung aus Kulanz angeboten. Voraussetzung hierfür war, dass eine Rückerstattung des abgebuchten Betrags bankseitig abgelehnt wurde.

11. inwiefern im Vorfeld zu Fragen der Cybersicherheit die Cybersicherheitsagentur konsultiert wurde sowie ggf. warum nicht;

12. welche Rückmeldungen ggf. seitens der Cybersicherheitsagentur erfolgten sowie möglicherweise (nicht) umgesetzt wurden;

Zu 11. und 12.:

Die Ziffern 11 und 12 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet. Die CSBW, die 2021 gegründet wurde und seit Anfang 2022 als eigenständige Landesoberbehörde tätig ist, wurde vom Landesmarketing in Bezug auf den Onlineshop vor Bekanntwerden des Sicherheitsvorfalls nicht konsultiert. Das Setup des Onlineshops erfolgte zum Kampagnenstart von THE LÄND Ende des Jahres 2021 in Zusammenarbeit mit der Werbeagentur, die die Kampagne und ihre verschiedenen Plattformen zu diesem Zeitpunkt inhaltlich und technisch betreute. In der Auswahl der Dienstleister und im Setup-Prozess wurden strenge IT-Sicherheitsmaßstäbe angelegt. Zu diesem Zeitpunkt lagen nach eingehender Prüfung keine Anhaltspunkte dafür vor, dass die gewählte Shop-Software technische Sicherheitslücken aufweist. Mit dem Anbieter der Shop-Software wurde ein Auftragsverarbeitungsvertrag abgeschlossen, der die DSGVO-konforme Verarbeitung von Daten sicherstellen soll und den Software-Anbieter zum Schutz der Daten, insbesondere vor unberechtigten Zugriffen Dritter, verpflichtet.

Zum Zeitpunkt der Inbetriebnahme des Onlineshops war dem Landesmarketing das Angebot der sich zu diesem Zeitpunkt im Aufbau befindlichen CSBW im Hinblick auf eine IT-Sicherheitstechnische Beratung noch nicht bekannt.

13. inwiefern sie neben dem THE LÄND-Onlineshop weitere Onlineshops betreibt (bitte ggf. mit konkreter Darstellung der jeweiligen Onlineshops);

Zu 13.:

Die Landesministerien betreiben neben dem THE LÄND-Onlineshop keine weiteren Onlineshops. Eine vollständige Erhebung der im nachgeordneten Bereich eingerichteten Onlineshops war in der zur Verfügung stehenden Zeit nicht möglich.

14. wie sie das Risiko für Sicherheitslücken in diesen unter Ziffer 13 dargestellten Onlineshops bewertet;

Zu 14.:

Onlineshops sind aufgrund ihrer ständigen Erreichbarkeit und der Verarbeitung sensibler Daten grundsätzlich potenziellen Sicherheitsrisiken ausgesetzt. Bei der vorgefundenen Sicherheitslücke im Shopsystem des Onlineshops von THE LÄND handelt es sich um eine sogenannte Zero-Day-Schwachstelle, die eine besondere Kategorie von Sicherheitslücken darstellt. Da sie dem Hersteller oder Betreiber und auch Anbietern von Sicherheitssoftware bzw. von Software zur Schadcode-Erkennung zum Zeitpunkt ihrer Ausnutzung noch nicht bekannt sind, ist ein vollständiger präventiver Schutz gegen deren Ausnutzung nicht möglich. Entsprechende Sicherheitslücken, die bei unmittelbar aus dem Internet erreichbaren Systemen auftreten und die zuerst von potenziellen Schädigern entdeckt werden, entziehen sich klassischen Präventionsmaßnahmen.

Generell gilt für Shop-Software – wie für andere Software ebenfalls – dass ein Schwachstellen- und Patch-Management umgesetzt und regelmäßige Updates installiert werden müssen. Zugänge sollten mit einer Multi-Faktor-Authentisierung abgesichert sein, ein Rechte- und Rollenkonzept für den Datenzugriff muss bestehen. Für diese Maßnahmen sollte ein Security-by-Design-Ansatz schon in der Konzeptionsphase umgesetzt werden. Außerdem empfiehlt die CSBW, Web-Angebote regelmäßig Schwachstellenscans zu unterziehen und für besonders kritische Anwendungen Penetrationstests durchzuführen. Sie erweitert darum aktuell ihr Angebot um einen Service, mit dem die öffentlichen Stellen des Landes entsprechende Leistungen über die CSBW insbesondere für aus dem Internet erreichbaren Systeme beauftragen können. Diesen Service hat die CSBW dem Staatsministerium für den Relaunch des Shop-Systems angeboten.

Insgesamt lässt sich festhalten, dass Sicherheitslücken bei Onlineshops ein grundsätzlich kalkulierbares Risiko darstellen, das durch technische und organisatorische Maßnahmen wirksam reduziert werden kann.

15. welche Konsequenzen sie aus dem Cyberangriff auf den THE LÄND-Onlineshop zieht.

Zu 15.:

Das Staatsministerium bedauert sehr, dass es trotz sehr hoher Sicherheits- und Sorgfaltsmaßnahmen zu dem Cybersicherheitsvorfall kommen konnte.

Das bislang genutzte Shop-System wird nicht weiterverwendet. Derzeit werden hierfür verschiedene Alternativen untersucht. Bis zur Einrichtung eines neues Shop-Systems bleibt der FÄNSHOP außer Betrieb.

Der Cyberangriff wird derzeit in Zusammenarbeit mit den Strafverfolgungsbehörden und der CSBW umfassend aufgearbeitet und aufgeklärt. Darüber hinaus prüft das Staatsministerium, welche zusätzlichen Maßnahmen ergriffen werden können, um das Risiko eines Angriffs so weit wie möglich zu reduzieren. Hierfür wird insbesondere der Ergebnisbericht der forensischen Untersuchung der ermittelnden Behörden abgewartet.

Haßler

Staatssekretär