

## **Antrag**

**der Abg. Dr. Hans Ulrich Rülke und  
Daniel Karrais u. a. FDP/DVP**

**und**

## **Stellungnahme**

**des Ministeriums für Finanzen**

### **Hackerangriff auf die L-Bank bzw. deren Dienstleister**

Antrag

Der Landtag wolle beschließen,  
die Landesregierung zu ersuchen  
zu berichten,

1. inwiefern es Ende Juli zu einem Hackerangriff auf die L-Bank bzw. deren Dienstleister im Zusammenhang mit der Abwicklung der Coronasoforthilfe gekommen ist;
2. wie viele Nutzer mit welchen in die Hände Dritter gelangten Informationen von diesem Hackerangriff betroffen waren;
3. was die Landesregierung bzw. die L-Bank unternommen hat, um die betroffenen Nutzer zu informieren und den Schaden zu minimieren;
4. welche Schäden genau entstanden sind – bei der L-Bank, dem Dienstleister oder den Nutzern;
5. inwiefern der Dienstleister, der angegriffen wurde, dadurch schadensersatzpflichtig gegenüber der L-Bank, der Landesregierung oder den Nutzern wurde;
6. welche Konsequenzen die L-Bank für die weitere Zusammenarbeit mit diesem Dienstleister gezogen hat;
7. welche Auswirkungen dies für die – eh schon schwierige und mit vielen Problemen versehene – weitere Abwicklung der Coronasoforthilfe hat;

8. inwiefern andere Förderprogramme der L-Bank und/oder andere Dienstleister ebenfalls von diesem Angriff betroffen waren (ggf. wieder mit Informationen zur Anzahl der betroffenen Nutzerinnen und Nutzer und den in die Hände Dritter gelangten Informationen);
9. wie viele erfolgreiche und nicht-erfolgreiche Hackerangriffe allgemein es in den letzten drei Jahren auf die L-Bank gab;
10. welche Daten von wie vielen Nutzern dabei betroffen waren;
11. wie sie allgemein die Cybersicherheit der L-Bank und deren Dienstleistern bewertet, insbesondere inwiefern hier Handlungsbedarf besteht und die bankenrechtlichen Besonderheiten gewährt sind.

14.8.2024

Dr. Rülke, Karrais, Birnstock, Bonath, Fink-Trauschel, Haag,  
Haußmann, Dr. Jung, Reith, Scheerer, Dr. Schweickert FDP/DVP

#### Begründung

Laut einer E-Mail an Empfänger der Coronasoforthilfe kam es Ende Juli zu einem erfolgreichen Hackerangriff auf die L-Bank bzw. deren Dienstleister. Dabei sind wohl Zugänge kompromittiert worden und nicht-autorisierte Daten in die Hände Dritter gelangt. Die Antragsteller erkundigen sich nach dem genauen Ausmaß sowie den Konsequenzen des Hackerangriffs.

#### Stellungnahme

Mit Schreiben vom 5. September 2024 Nr. FM5-3212-113/3 nimmt das Ministerium für Finanzen auf Basis einer Stellungnahme der L-Bank zu dem Antrag wie folgt Stellung:

*Der Landtag wolle beschließen,  
die Landesregierung zu ersuchen  
zu berichten,*

*1. inwiefern es Ende Juli zu einem Hackerangriff auf die L-Bank bzw. deren Dienstleister im Zusammenhang mit der Abwicklung der Coronasoforthilfe gekommen ist;*

Zu 1.:

Es gab einen Sicherheitsvorfall bei einem von der L-Bank für das Hosting einer Online-Anwendung beauftragten Dienstleister, bei dem Daten abgeflossen sind.

*2. wie viele Nutzer mit welchen in die Hände Dritter gelangten Informationen von diesem Hackerangriff betroffen waren;*

Zu 2.:

Es sind L-Bank-Login-Daten für die Online-Anwendung für das Rückmeldeverfahren Coronahilfen von möglicherweise bis zu 25 700 Kundinnen und Kunden in die Hand unbefugter Dritter gelangt.

*3. was die Landesregierung bzw. die L-Bank unternommen hat, um die betroffenen Nutzer zu informieren und den Schaden zu minimieren;*

Zu 3.:

Nach Abschluss einer für die Kundenbelange hinreichenden Klärung wurden die möglicherweise betroffenen 25 700 Kundinnen und Kunden am 9. August 2024 mit dem beiliegenden Anschreiben über den Datenabfluss informiert.

*4. welche Schäden genau entstanden sind – bei der L-Bank, dem Dienstleister oder den Nutzern;*

Zu 4.:

L-Bank-Login-Daten der Kundinnen und Kunden sind in die Hand unbefugter Dritter gelangt. Diese bestehen zum einen aus der Kennung (einer E-Mail-Adresse der Kundinnen/Kunden) sowie zum anderen aus dem dazugehörigen Passwort. Die Passwörter sind hochverschlüsselt. Es gibt derzeit keinerlei Hinweise auf den Abfluss von weiteren Daten. Bei der L-Bank sind keine Schäden entstanden. Über Schäden bei dem Dienstleister oder den betroffenen Nutzerinnen und Nutzern ist der L-Bank nichts bekannt.

*5. inwiefern der Dienstleister, der angegriffen wurde, dadurch schadensersatzpflichtig gegenüber der L-Bank, der Landesregierung oder den Nutzern wurde;*

Zu 5.:

Mangels aktuell bekannter Schäden stellt sich diese Frage derzeit nicht.

*6. welche Konsequenzen die L-Bank für die weitere Zusammenarbeit mit diesem Dienstleister gezogen hat;*

Zu 6.:

Die L-Bank und ihr Dienstleister haben unmittelbar nach Bekanntwerden des Vorfalls operative Schutzmaßnahmen wie Trennung der Server, erweiterte Monitorings und Sonderuntersuchungen durchgeführt. Die L-Bank arbeitet mit diesem Dienstleister nicht mehr zusammen.

*7. welche Auswirkungen dies für die – eh schon schwierige und mit vielen Problemen versehene – weitere Abwicklung der Coronasoforthilfe hat;*

Zu 7.:

Der Vorfall hat keine Auswirkungen auf die Coronasoforthilfen. Die betroffene Online-Anwendung der L-Bank für das Rückmeldeverfahren Coronahilfen wurde zum 31. Juli 2024 planmäßig abgeschaltet. Die Abschaltung hat mit dem Vorfall nichts zu tun und war schon lange geplant. Es gab keinen Zugriff unberechtigter Dritter auf die weiteren Daten in der Online-Anwendung der L-Bank.

*8. inwiefern andere Förderprogramme der L-Bank und/oder andere Dienstleister ebenfalls von diesem Angriff betroffen waren (ggf. wieder mit Informationen zur Anzahl der betroffenen Nutzerinnen und Nutzer und den in die Hände Dritter gelangten Informationen);*

Zu 8.:

Es sind nur die Coronasoforthilfen und die Härtefallhilfen (Energie-KMU) betroffen.

*9. wie viele erfolgreiche und nicht-erfolgreiche Hackerangriffe allgemein es in den letzten drei Jahren auf die L-Bank gab;*

*10. welche Daten von wie vielen Nutzern dabei betroffen waren;*

Zu 9. und 10.:

Bei der L-Bank gab es keine weiteren erfolgreichen und identifizierten Hackerangriffe.

Es waren auch keine weiteren Daten betroffen.

*11. wie sie allgemein die Cybersicherheit der L-Bank und deren Dienstleistern bewertet, insbesondere inwiefern hier Handlungsbedarf besteht und die bankenrechtlichen Besonderheiten gewährt sind.*

Zu 11.:

Die L-Bank ist über die Vorgaben des Kreditwesengesetzes (KWG), den Mindestanforderungen an das Risikomanagement (MaRisk) und daraus abgeleitet den bankaufsichtlichen Anforderungen an die IT (BAIT) verpflichtet, einen IT-Sicherheitsstandard zu implementieren. Die Bank hat sich, wie viele andere Behörden auch, für das BSI Grundsatzkompendium des Bundesamts für Sicherheit in der Informationstechnik als IT-Sicherheitsstandard entschieden. Die L-Bank verbessert kontinuierlich ihre Cybersicherheit und ist derzeit in der Umsetzung der Anforderungen aus dem Digital Operational Resilience Act der EU (DORA).

Öffentlich verfügbare IT-Security-Ratings bestätigen der L-Bank und den durch Dienstleister für sie betriebenen IT-Anwendungen ein gutes Schutzniveau.

Dr. Splett

Staatssekretärin

**Sehr geehrte Kundinnen und Kunden,**

wir möchten Sie heute über zwei wichtige Themen informieren.

Nach Abschluss des Rückmeldeverfahrens ist die Online-Anwendung planmäßig zum 31. Juli 2024 abgeschaltet worden. Hierauf wurde in der Online-Anwendung hingewiesen. Bitte beachten Sie, dass damit auch die entsprechenden Funktionen nicht mehr zur Verfügung stehen.

Kurz bevor die Anwendung abgeschaltet wurde, sind trotz der sehr hohen Sicherheitsvorkehrungen bei der L-Bank und den von ihr beauftragten Dienstleistern bei einer Hackerattacke auf einen Dienstleister Daten abgeflossen. Dabei ist möglicherweise Ihr L-Bank-Login-Name und das Passwort in verschlüsselter Form an unbefugte Dritte gelangt.

Uns ist wichtig zu betonen, dass für darüberhinausgehende Daten keine unmittelbare Gefahr bestand: Ihre persönlichen Daten bei der L-Bank waren weiterhin durch die Verschlüsselung sowie eine 2-Faktor-Authentifizierung geschützt. Inzwischen sind die Passwörter aufgrund der Abschaltung der Online-Anwendung zudem nicht mehr nutzbar.

**Da uns der Schutz Ihrer persönlichen Daten sehr wichtig ist, möchten wir Sie vorsorglich auf Folgendes hinweisen: Sollten Sie dasselbe Passwort auch bei anderen Online-Diensten verwendet haben, empfehlen wir Ihnen, dort die Passwörter zu ändern. Es handelt sich dabei lediglich um eine Vorsorgemaßnahme, da die entwendeten Passwörter verschlüsselt sind.**

Wichtige Hinweise zur Passwortsicherheit finden Sie auf der [Internetseite des Bundesamtes für Sicherheit in der Informationstechnik \(BSI\)](#).

Wir möchten uns an dieser Stelle für etwaig entstehende Unannehmlichkeiten entschuldigen.

Sollten Sie noch Fragen haben, wenden Sie sich bitte unter Angabe Ihrer Vorgangsnummer per E-Mail an [rueckmeldeverfahren-soforthilfe@l-bank.de](mailto:rueckmeldeverfahren-soforthilfe@l-bank.de) oder rufen Sie unsere Hotline unter 0721/150-2900 an.

Mit freundlichen Grüßen

Ihre L-Bank

Internet:  
<https://www.l-bank.de/>

**Landeskreditbank Baden-Württemberg – Förderbank – (L-Bank)**

Anstalt des öffentlichen Rechts

Schlossplatz  
76113 Karlsruhe

Handelsregister Mannheim HRA 104441

Vorstand:

Edith Weymayr, Vorsitzende

Dr. Iris Reinelt

Johannes Heinloth

**Datenschutz**

In unserer E-Mail finden Sie einen externen Link auf die Internetseite eines Dritten. Auf den Inhalt dieser Website haben wir keinen Einfluss und können daher keine Gewähr übernehmen. Für die Inhalte der verlinkten Seite ist der jeweilige Betreiber verantwortlich.