

Questions and answers regarding the cyber-attack

1. Was V-Bank the target of a cyber-attack?

Unfortunately, yes. According to the current state of knowledge, the unauthorised access to data was specifically directed against a service provider that processes data on behalf of V-Bank.

2. How did V-Bank respond to the incident?

We are well prepared for such a scenario and promptly set up a task force of internal and external experts specialising in cybercrime to manage the incident and investigate it thoroughly. We informed the relevant supervisory and law enforcement authorities immediately and will be filing a complaint and pressing charges.

3. Has client data been affected by the incident?

Yes, unfortunately, client data has been compromised. Based on information currently available, this includes the following data categories: account holders' names, dates of birth and contact details (postal addresses, e-mail addresses, telephone numbers), account-related information, in particular asset status, transaction data and reference accounts.

4. Have any login or tax details been affected by the incident?

No. Our security systems responded immediately. We can therefore confirm that the perpetrators did not have access to any V-Bank accounts or securities accounts at any time. This also applies to all account access data (usernames and passwords), as well as tax details. This ensures that no funds, securities or crypto-assets were misappropriated at any time.

5. What impact has the incident had on V-Bank's systems?

V-Bank's systems, such as online banking, have not been affected by the incident and remain fully operational, with the customary high security standards in place.

6. Can I still communicate securely with V-Bank?

Yes. You can continue to communicate with us via telephone, e-mail or our online services, with the same high security standards as always. These systems were not affected by the attack.

7. Who at V-Bank should I contact if I have any questions or concerns?

Please contact our client service team with any questions you may have. You can contact our client service team by telephone at: +49 (89) 740800-0.

8. What can I do now?

We would ask you to be particularly vigilant in the coming days, especially if you notice any suspicious activity, are contacted by unknown third parties, or by people claiming to be employees of V-Bank or our business partners. If in doubt, please verify any suspicious enquiries confirmed by telephone with your contacts at V-Bank or our business partners before responding to them.

9. What action is V-Bank taking in response to this incident?

Our immediate priority is to protect our clients' data, assets and reputation. All findings from the investigation are being promptly incorporated into a comprehensive review and, where necessary, into the further development of our security architecture.

10. Should I expect my data to be made public?

Unfortunately, although we currently have no indication that this will happen, we cannot rule it out. As of 22 June 2026, 17:00 hrs., we have no information to suggest that any data has been published. We are monitoring the situation on an ongoing basis.

11. What action is V-Bank going to take to prevent the affected data from being published?

Unfortunately, the data is no longer within V-Bank's control. We are therefore unable to rule out the possibility of disclosure.

12. Who is the service provider in question? What services does it provide to V-Bank?

The service provider in question is a certified IT service provider that provides cloud services to V-Bank.

13. Why did the service provider in question have V-Bank's client data in its possession?

The service provider did not hold any client data. It had access to an externally hosted V-Bank database, as required to perform its services. This database is separate from the core banking system.