V BANK

Die Vermögensbank.

Fragen und Antworten zum Cyber-Angriff

Die nachfolgenden Q&A basieren auf dem Ergebnis der kundenspezifischen forensischen Analyse am 03.07.2026 (18:00 Uhr). Die Angaben sind nach bestem Wissen und Gewissen erstellt.

1. Wurde die V-Bank zum Ziel einer Cyber-Attacke?

Leider ja, der illegale Datenzugriff richtete sich nach aktuellem Kenntnisstand gezielt gegen einen Dienstleister, der im Auftrag der V-Bank Daten einsetzt.

2. Wie hat die V-Bank auf den Vorfall reagiert?

Wir waren auf ein solches Szenario gut vorbereitet und hatten umgehend eine Taskforce aus internen und externen, auf Cyber-Kriminalität spezialisierten Experten eingerichtet, um den Vorfall in einer ersten Reaktionsphase zu bewältigen und gründlich zu untersuchen. Mittlerweile haben wir die zweite Reaktionsphase mit dem Neuaufbau des betroffenen IT-Systems gestartet. Die zuständigen Aufsichts- und Strafverfolgungsbehörden hatten wir umgehend informiert und stehen im ständigen Austausch. Einen Strafantrag haben wir gestellt.

3. Sind Kundendaten von dem Vorfall betroffen?

Ja, bedauerlicherweise sind Kundendaten abgeflossen. Dabei handelt es sich nach aktuellem Erkenntnisstand um folgende Datenkategorien: Namen von Kontoinhaberinnen und -inhabern, Geburtsdaten sowie Kontaktinformationen, (Postanschriften, E-Mail-Adressen, Telefonnummern), kontobezogene Informationen, insbesondere Vermögensstatus, Transaktionsdaten, technische Benutzerkennungen und Referenzkonten.

Die Detailanalyse der hinzugezogenen Forensiker hat ergeben, dass über die oben genannten Datenkategorien hinaus auch Ausweisdaten und die Steueridentifikationsnummer (Steuer-ID) entwendet wurden. Hierzu werden die Kunden je nach Betroffenheit noch individuell informiert.

4. Sind Zugangsdaten von dem Vorfall betroffen?

Der eigentliche Schutz des Kontos resultiert aus der Kombination eines Wissensfaktors (PIN bzw. Passwort) mit einem Besitzfaktor (Airlock App). Aus der alleinigen Kenntnis der Benutzerkennung ist kein Zugriff auf das Konto möglich.

Das Ende der forensischen Analyse hat ergeben, dass Passwörter vom Datenzugriff nicht betroffen waren. Somit ist die Absicherung weiterhin intakt und ein ausreichender Schutz ist gegeben.

5. Welche Auswirkungen hat der Vorfall auf die Systeme der V-Bank?

Die Systeme der V-Bank wie das Onlinebanking sind von dem Vorfall nicht betroffen und stehen weiterhin in vollem Umfang und mit den gewohnt hohen Sicherheitsstandards zur Verfügung.

6. Kann ich noch sicher mit der V-Bank kommunizieren?

Ja. Sie können weiterhin mit den gewohnt hohen Sicherheitsstandards via Telefon, E-Mail oder unseren Online-Services mit uns kommunizieren. Diese Systeme waren vom Angriff nicht betroffen.

7. An wen bei der V-Bank kann ich mich bei Fragen oder Bedenken wenden?

Sie können sich mit Ihren Fragen an unsere Kundenbetreuung wenden. Telefonisch erreichen Sie unsere Kundenbetreuung unter: +49 (89) 740800-0.

8. Was kann ich jetzt tun?

Wir bitten Sie, in der nächsten Zeit um erhöhte Aufmerksamkeit, insbesondere falls Sie verdächtige Aktivitäten wahrnehmen, von unbekannten Dritten kontaktiert werden oder von Personen, die sich als vermeintliche Mitarbeiter der V-Bank oder unserer Geschäftspartner ausgeben. Lassen Sie verdächtige Anfragen im Zweifel von Ihren Ansprechpartnern bei der V-Bank oder unseren Geschäftspartnern telefonisch bestätigen, bevor Sie darauf reagieren.

9. Welche Konsequenzen zieht die V-Bank aus diesem Vorfall?

Unsere höchste Priorität gilt dem Schutz der Daten, Vermögenswerten und der Reputation unserer Kunden. Alle Erkenntnisse aus den Ermittlungen fließen unmittelbar in eine umfassende Überprüfung und falls erforderlich in die Weiterentwicklung unserer Sicherheitsarchitektur ein. Wir haben das Monitoring bereits erweitert und zusätzliche Sicherheitsmaßnahmen installiert. In den nächsten Wochen werden wir das grundsätzliche Sicherheitskonzept unabhängig überprüfen lassen und Empfehlungen aus diesem Review umsetzen. Der Vorfall hat gezeigt, dass unsere Sicherheitssysteme im Kernbanksystem unmittelbar reagiert haben. Die Täter hatten zu keinem Zeitpunkt Zugriff auf Konten/Depots der V-Bank. Ein Abfluss von Vermögen hat nicht stattgefunden.

10. Muss ich damit rechnen, dass meine Daten veröffentlicht werden?

Eine Veröffentlichung der Daten können wir leider nicht ausschließen. Aufgrund unserer Überwachung des Darknets (Identity Monitoring) nach Hinweisen zu dem Vorgang liegen uns mit Stand vom 03.07.2026, 18:00 Uhr, keine Erkenntnisse vor, dass die Daten veröffentlicht wurden. Wir überwachen weiter engmaschig mit externen Experten für Cyber-Vorfälle das Darknet.

11. Was tut die V-Bank, um eine Veröffentlichung zu verhindern?

Die Daten haben den Einflussbereich der V-Bank leider verlassen. Eine Veröffentlichung können wir daher leider nicht ausschließen.

12. Wieso befand sich der Dienstleister im Besitz von Kundendaten der V-Bank?

Der Dienstleister befand sich nicht im Besitz von Kundendaten. Er hatte einen für seine Dienstleistungen notwendigen Zugriff auf eine extern gehostete Datenbank der V-Bank. Diese ist vom Kernbanksystem getrennt.

13. Was passiert, wenn jemand mit der Steuer-ID illegalerweise eine Steuerklärung abgibt, Leistungen gegenüber Behörden beantragt oder allgemein diese Information nutzt, um glaubhaft zu machen, dass er tatsächlich der Inhaber der Steuer-ID ist.

In der Regel ist eine Steuer-ID allein nicht ausreichend, um diese Dinge durchzuführen.
Vorsorglich können Sie folgendes tun:

- Kontaktieren Sie Ihr zuständiges Wohnsitzfinanzamt schriftlich oder über das ELSTER-Portal. Teilen Sie dem Amt mit, dass Ihre steuerlichen Daten gestohlen wurden. Das Finanzamt vermerkt dies in Ihrer Steuerakte als Sperr- oder Prüfvermerk. Dadurch werden eingehende Steuererklärungen oder Anträge auf Steuerrückerstattung besonders streng manuell geprüft, um Missbrauch zu verhindern.
- Informieren Sie die SCHUFA über den Identitätsdiebstahl. Die Schufa setzt ein Warnkennzeichen in Ihre Akte. Vertragspartner (wie Banken oder Mobilfunkanbieter) prüfen Neuanträge dann besonders gründlich.