D-Trust GmbH | 10969 Berlin

D-Trust GmbH
Kommandantenstraße 15
10969 Berlin

Telefon +49 (0)30 25 93 91-0
Telefax +49 (0)30 25 93 91-22
E-mail info@d-trust.net

www.d-trust.de

Abschlussinformation Datenschutzvorfall D-Trust GmbH

Datum
03.04.2025

Telefon
+49 (0)30 25 93 91-0

Sehr geehrte Damen und Herren,

in den vergangenen Wochen haben wir Sie über den Datenschutzvorfall im Antragsportal für Signatur- und Siegelkarten der D-Trust GmbH informiert. Mit der folgenden abschließenden Stellungnahme möchten wir Ihnen die Gelegenheit geben, den Hergang und die anschließende Behandlung des Vorfalls in einem zusammenfassenden Dokument nachzuvollziehen. Darüber hinaus möchten wir Ihnen einen Ausblick zu den geplanten nächsten Schritten geben.
Vorab möchten wir uns hiermit für die entstandenen Umstände, die Ihnen und Ihren Mitgliedern bzw. Kunden entstanden sind, ausdrücklich entschuldigen.

Zusammenfassung des Datenschutzvorfalls

Die D-Trust GmbH wurde vom 1. bis 6. Januar 2025 Ziel eines Angriffs auf das D-Trust-Antragsportal. Er wurde am 13. Januar 2025 im Rahmen eines Betriebs-Routinechecks festgestellt. Der Angriff betraf die Antragsdaten, d. h. die von den Betroffenen im Rahmen ihrer Antragsprozesse eingegebenen Daten. Diese Daten konnten aus dem Antragsbearbeitungssystem ausgelesen und möglicherweise abgerufen werden. Bei den abgerufenen Daten handelt es sich um personenbezogene Daten wie etwa Vor- und Nachname, E-Mail-Adresse, Geburtsdatum und in einigen Fällen Adress- und

Sitz der Gesellschaft: Berlin
Handelsregister:
AG Berlin-Charlottenburg
HRB 74346
USt-IdNr.: DE 202620438

Geschäftsführer:
Markus Bleher
Jochen Felsner

Deutsche Bank AG
BIC: PBNKDEFFXXX
IBAN: DE67 1001 0010 0631 0311 00

Teil der Bundesdruckerei-Gruppe

Ausweisdaten. Weiterhin gilt: ausgegebene Karten (Signatur- und Siegelkarten, eHBA oder SMC-B) wurden nicht kompromittiert und können weiter genutzt werden. PINs, Passwörter, Login-Daten, Zahlungsinformationen sowie andere Systeme waren ebenfalls nicht betroffen.

Sofortmaßnahmen und Kommunikation

Unmittelbar nach Entdecken des Vorfalls sind umfassende Sofortmaßnahmen ergriffen worden, um den Schutz der Daten im Portal sicherzustellen. Die Daten- und Ausmaßanalyse wurde gestartet, um festzustellen, welche Antragssteller konkret betroffen sind. Die zuständigen Aufsichtsbehörden (Datenschutz, Bundesnetzagentur, BSI wurden fristgerecht informiert und ein spezialisiertes IT-Sicherheitsteam aus internen und externen Experten wurde eingesetzt, um die Hintergründe und Auswirkungen des Vorfalls zu analysieren. Die potenziell betroffenen Kunden der D-Trust wurden auf Basis der Ausmaßanalyse informiert. Je nach vertraglicher Vorgabe fand dies in direkter Ansprache durch die D-Trust oder die zuständigen Organisationen statt. Darüber hinaus wurde Strafanzeige gegen Unbekannt beim LKA Berlin gestellt und die Öffentlichkeit informiert.

Am 23. Januar 2025, mehr als drei Wochen nach dem Angriff auf das D-Trust Antragsportal, erhielt die D-Trust ein Schreiben des Chaos Computer Clubs (CCC), in dem der Verein die Verantwortung für den Angriff auf das Antragsportal für Signatur- und Siegelkarten der D-Trust einem „anonymen Sicherheitsforscher" zuschreibt. Das von der Bundesdruckerei-Gruppe für solche Fälle bereitgestellte Hinweissystem wurde allerdings seitens des Sicherheitsforschers nicht genutzt. Laut des Schreibens des CCC seien die ausgelesenen Daten durch den Angreifer im Nachgang gelöscht worden. Nach Angaben des CCC bestand also nicht die Gefahr eines Datenmissbrauchs.

Weitergehende Maßnahmen

Ursächlich für die Schwachstelle war ein singulärer Software-Fehler, der zu einer unzureichenden Zugriffskontrolle der Anwendung führte. Im Nachgang des Datenschutzvorfalls haben wir kurzfristige Maßnahmen ergriffen sowie in Abstimmung mit den zuständigen Aufsichtsbehörden und der beauftragten Konformitätsbewertungsstelle ein umfangreiches Maßnahmenpaket definiert, um sicherzustellen, dass eine derartige Schwachstelle zukünftig nicht mehr auftritt. Die Maßnahmen reichen unter anderem von der Spezifizierung des Code Reviews über die Ausweitung der automatisierten Schwachstellenanalyse, die Überarbeitung des Penetration Testing-Programms bis hin zum Ausbau des Security Monitorings und der Schulungs- und Trainingsmaßnahmen. Diese Maßnahmen steigern nicht nur die Sicherheit im Rahmen der Softwareentwicklung, sondern werden das Sicherheitsniveau insgesamt noch einmal optimieren. Auch während der Umsetzung

der Maßnahmen stehen wir in regelmäßigem Kontakt mit den Aufsichtsbehörden und der verantwortlichen Konformitätsbewertungsstelle.

Neben den genannten Maßnahmen stehen wir im direkten Austausch mit der Bundesärztekammer, der Bundeszahnärztekammer, der Apothekerkammer sowie verschiedenen regionalen Kammern. Es wurden Feedback-Runden durchgeführt sowie ein Lessons Learned-Workshop mit der gematik. Ein weiterer Workshop mit der Bundesärztekammer steht noch aus. Zielsetzung dieser Runden war und ist im Wesentlichen die Verbesserung von Prozessen und Kommunikationsabläufen, um diese reibungsloser und zuverlässiger zu gestalten.

An dieser Stelle möchten wir uns noch einmal herzlich für die enge Kooperation, Ihre Unterstützung und Ihr Verständnis in den letzten Monaten bedanken!

Markus Bleher

Dokument unterschrieben
von: Markus Bleher
am: 04.04.2025 11:00

Jochen Felsner

2025.04.04 16:15:39 +02'00'

Markus Bleher
Geschäftsführer

Jochen Felsner
Geschäftsführer