



Sicherheitsvorfall 2025

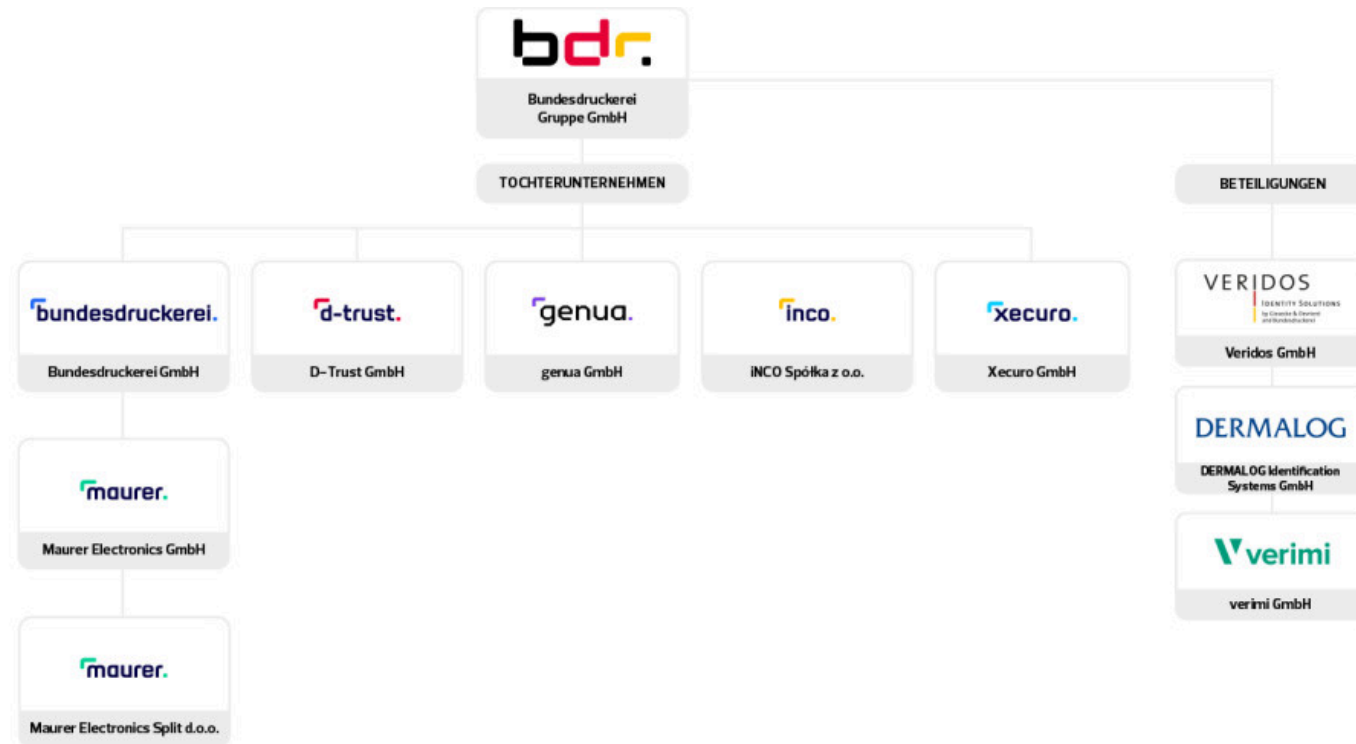
Theo Leuthardt

Modul: IT-Sicherheit

01

Wer ist die D-Trust?

Wer ist die D-Trust?



Qualifizierter Vertrauensdiensteanbieter gemäß eIDAS-Verordnung (seit 2016)

Produkte: Digitale Zertifikate, elektronische Signaturen, eHBA, SMC-B-Ausweise

02

Der Vorfall

Der Vorfall

13. Januar 2025

Angriff auf das Antragsportal für Signatur- und Siegelkarten `portal.d-trust.net`

Was geschah?

Eine **API-Schnittstelle** des Portals war völlig ungeschützt — ohne Authentifizierung oder Zugangskontrolle. Durch simples Durchnummerieren von Antrags-IDs (**IDOR**) konnten alle Datensätze abgerufen werden.

Wer steckt dahinter?

Ein **White-Hat-Hacker** entdeckte die Schwachstelle und meldete sie an den **CCC** – nicht direkt an D-Trust, aus Angst vor **§ 202a StGB**.

Chaos Computer Club (CCC): „Kombination aus Versehen, Inkompetenz und mangelnder Sorgfalt.“
Keine aufwändigen Schutzmechanismen wurden umgangen – die Daten waren faktisch ungeschützt.

03

Betroffene Kunden & Daten

Betroffene Kunden & Daten

Entwendete Daten

- Vor- und Nachname
- E-Mail-Adresse
- Telefonnummer
- Geburtsdatum
- Teilweise Adressdaten
- Teilw. Ausweisdaten (Dokumentennr., Gültigkeitsdatum, Behörde)

Nicht betroffene Daten

- Login-Daten / Passwörter
- PINs
- Zahlungsinformationen
- Ausgegebene Signatur-/Siegelkarten

Betroffene Personengruppen:

- Ärzt:innen & Psychotherapeut:innen (über Landesärztekammern & KVen)
- Apotheker:innen (über Apothekerkammern)
- Alle, die einen **eHBA** oder **SMC-B** beantragt hatten

04

Konsequenzen

Reaktion & Kritik

Reaktion von D-Trust

- Sofortige Sicherung des Portals
- Benachrichtigung der Aufsichtsbehörden
- Zusammenarbeit mit IT-Sicherheitsteam
- Information der Betroffenen
- **Strafanzeige gegen Unbekannt**

CCC: 5-Punkte-Plan

1. Verantwortung übernehmen
2. Förmliche Entschuldigung
3. Zeitgemäße Sicherheitsstandards
4. Hackerparagraphen abschaffen
5. Empfindliche Strafe durch BfDI

Der CCC warf D-Trust vor, mit „bedeutungsschwangerer Cyber-Rhetorik“ von der eigenen Verantwortung ablenken zu wollen.

Auswirkungen

Für Betroffene

Erhöhtes Risiko für **Phishing & Identitätsdiebstahl** durch Kombination sensibler Daten.

Für D-Trust / BDr

Reputationsschaden & mögliche **DSGVO-Bußgelder** (Art. 33/34).

Für Gesundheitswesen

Vertrauensverlust in die Telemetrieinfrastruktur – kurz vor Einführung der **ePA 3.0**.

05

Präventionsmaßnahmen

Präventionsmaßnahmen

Technisch

- **API-Sicherheitsaudits & Pentests**
- Authentifizierung & **Datenminimierung**
- Echtzeit-**Monitoring**

Organisatorisch

- **Responsible-Disclosure- / Bug-Bounty-Programm**
- Klarer **Incident-Response-Plan**
- **Sicherheitsschulungen** für Entwickler

Regulatorisch

- Reform **§ 202a StGB** – Rechtssicherheit für Forscher
- Verbindliche Zertifizierungen für **KRITIS**-Anbieter
- Aufsichtsbehörden stärken

Kernproblem: Wer Lücken meldet, wird bestraft – wer sie ausnutzt, bleibt oft unentdeckt.

Quellen

Quelle	Link
D-Trust GmbH – Offizielle Meldung	d-trust.net
Chaos Computer Club – Stellungnahme & 5-Punkte-Plan	ccc.de
Heise Online – CCC spricht von „Cyber-Augenwischerei“	heise.de
Security Insider – Cyberangriff auf D-Trust	security-insider.de
Ärztekammer Niedersachsen	aekn.de
Landesärztekammer Baden-Württemberg	aerztekammer-bw.de
KV Sachsen – Datenschutzvorfall	kvsachsen.de
Apothekerkammer Nordrhein	aknr.de
Pharmazeutische Zeitung – CCC-Stellungnahme	pharmazeutische-zeitung.de
DSGVO-Portal – Sicherheitsvorfalls-DB	dsgvo-portal.de

Bilder: Organigramm – bundesdruckerei.de

d-trust.

Vielen Dank für die Aufmerksamkeit

Fragen?

