# Abfluss von persönlichen Daten: Hintergründe und Sofortmaßnahmen

CSBW
CYBER SICHERHEITS AGENTUR
BADEN-WÜRTTEMBERG

Ob Datenlecks versehentlich oder vorsätzlich entstehen – sensible Informationen sind gefährdet und oft frei im Netz zugänglich.

Die häufigsten Ursachen für Datenlecks sind Sicherheitslücken, eine unzureichende Verschlüsselung bei der Übertragung oder die fehlerhafte Konfiguration eines Systems. Datenlecks können aber auch bei Cyberangriffen entstehen oder wenn sensible Daten fehlerhaft gehandhabt beziehungsweise Zugangsdaten versehentlich weitergegeben werden.

**Kriminelle nutzen Sicherheitslücken**
Kommt es auf Online-Plattformen zu Sicherheitsvorfällen, sind häufig die Daten der Nutzenden betroffen. Personenbezogene Daten wie Name, Anschrift, Geburtsdatum, Gesundheitsdaten oder Kontoinformationen gelangen so in die Hände Unbefugter.

Beim sogenannten Doxing sammeln Kriminelle personenbezogene Daten, bündeln diese und machen sie öffentlich verfügbar. Diese Daten können von Kriminellen für gezieltes Phishing, Betrugsversuche und für einen Identitätsdiebstahl genutzt werden. Mit Hilfe eines Identity Leak Checkers lässt sich prüfen, ob Daten in Datenlecks aufgetaucht sind.

**Schadensbegrenzung durch schnelles Eingreifen**
Nach der Entdeckung eines Datenlecks ist der betroffene Dienstleister gesetzlich verpflichtet, die Nutzenden zu informieren, deren Daten abgeflossen sind.

Bis ein Datenabfluss bemerkt wird, können die gestohlenen Informationen von Kriminellen bereits missbräuchlich verwendet werden. Die Folgen eines Datenabflusses zeigen sich häufig erst zeitversetzt. Wachsamkeit bleibt daher entscheidend.

**Prüftool: Identity Leak Checker**
Ob Ihre Daten bereits in bekannten Datenlecks aufgetaucht sind, können Sie mit dem **Identity Leak Checker des Hasso-Plattner-Instituts** prüfen.

## Empfehlung

**Ein wirksamer Schutz ist der bewusste und sparsame Umgang mit den eigenen Daten.**

- → Nur Daten preisgeben, die für den jeweiligen Zweck notwendig sind.
- → Privatsphäre-Einstellungen bei Sozialen Netzwerken und Messenger-Diensten prüfen.
- → Dateneingabe nur bei verschlüsselten Verbindungen.
- → Alte Konten und Profile löschen.

## Die wichtigsten Sofortmaßnahmen im Überblick:

**Passwörter umgehend ändern**
Nutzen Sie starke, einzigartige Passwörter und aktivieren Sie möglichst die Zwei-Faktor-Authentifizierung.

**Konten und Bankbewegungen prüfen**
Achten Sie auf verdächtige Aktivitäten bei E-Mail-, Social-Media- und Bankkonten.

**Betroffene Stellen informieren**
Banken, Kreditkartenanbieter oder andere relevante Dienste sollten unverzüglich informiert werden.

**Vorsicht vor Phishing**
Nach aufgetretenen Datenlecks steigt die Wahrscheinlichkeit für betrügerische E-Mails, SMS oder Anrufe deutlich an.

**Vorfälle dokumentieren**
Screenshots, E-Mails und verdächtige Nachrichten können später wichtig werden.

**Anzeige erstatten**
Informieren Sie bei Identitätsmissbrauch oder Betrug umgehend die Polizei.

Weitere Informationen unter:
**www.cybersicherheit-bw.de**

CSBW Prävention
Kontakt: schulungen@cybersicherheit.bwl.de
Stand: 08.2026