IDENTITÄTSDIEBSTAHL

Die Folgen für Betroffene und wie ihnen geholfen werden kann

April 2022

AK WIEN
GERECHTIGKEIT MUSS SEIN

Identitätsdiebstahl

Die Folgen für Betroffene und wie ihnen geholfen werden kann

April 2022

Studie im Auftrag der Arbeiterkammer

Inhalt

Inhalt

Einleitung

> Zu Beginn der meisten Cybercrime-Straftaten steht der Diebstahl einer digitalen Identität.[1]

Identitätsdiebstahl hat Konjunktur, es betrifft Unternehmen und Konsument:innen. Im Jahr 2019 gaben bereits rund elf Prozent der Österreicher:innen an, dass sie schon einmal von Identitätsdiebstahl betroffen waren.[2] Die Konsequenzen für Einzelne können massiv sein, denn die gestohlenen Daten werden für kriminelle Aktivitäten genutzt.

Die Daten werden z. B. missbraucht, um Bestellungen zu machen und Konten für Geldwäsche zu eröffnen. Ist jemand von Identitätsmissbrauch betroffen, beginnt ein mühsamer Prozess, um den Schaden zu minimieren. Die Folgen für Betroffene können einschneidend werden: sie kämpfen mit Anwaltskosten, Inkassobüros und psychischer Belastung.

Niemand ist vor Identitätsdiebstahl gefeit, denn von Wohnungssuche, Job-Bewerbungen, hin zur Nutzung von E-Mail-Accounts – die möglichen Eintrittsvektoren für Kriminelle sind breit gestreut. Umso wichtiger ist der Fokus auf die Prävention zur Verhinderung von Identitätsdiebstahl sowie auf die Begleitung von Betroffenen. Die potenziellen Handlungsansätze und Maßnahmen reichen von digitalen Identitätsverifizierungen hin zu Tools, die Plattformen selbst zur Detektion von Unregelmäßigkeiten nutzen. Dabei zeigt sich, dass bei Identitätsdiebstahl stets die Abwägung der Maßnahmen im Spannungsfeld von Sicherheit durch strengere Identitätsüberprüfungen und dem Recht auf Anonymität gesehen werden muss.

Die vorliegende Studie geht dem Phänomen Identitätsdiebstahl aus der Perspektive von Betroffenen nach.

Im 1. Kapitel („1. Die digitale Identität“ auf Seite 6) wird erklärt, welche Daten die digitale Identität einer Person ausmachen. Das 2. Kapitel („2. Wie gelangen Kriminelle an fremde Daten?“ auf Seite 8) beschreibt, wie Kriminelle an diese Daten gelangen. Im 3. Kapitel („3. Wofür werden gestohlene Daten missbraucht?“ auf Seite 12) wird erklärt, wofür Identitäten missbraucht werden.

Im 4. Kapitel („4. Welche Folgen hat Identitätsmissbrauch für Betroffene?“ auf Seite 15) werden die Folgen für Betroffene geschildert. Dem folgt eine Diskussion über Handlungsansätze und Maßnahmen in Kapitel 5 („5. Handlungsansätze und Maßnahmen“ auf Seite 17) und ein Ausblick im 6. Kapitel („6. Ausblick“ auf Seite 25) auf offene Fragestellungen und Forderungen.

Im 7. Kapitel („7. Wie kann ich mich gegen Identitätsmissbrauch schützen?“ auf Seite 26) wird anschaulich, wie Identitätsdiebstahl vorgebeugt werden kann. Im 8. Kapitel („8. Ich bin betroffen, was ist zu tun?“ auf Seite 27) sind praktische Tipps für Betroffene von Identitätsmissbrauch vermerkt.

1 BKA Deutschland (2020). Cybercrime. Bundeslagebild 2019. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2019.pdf

2 Statista (2020). Umfrage zu Identitätsdiebstahl in Österreich. https://de.statista.com/statistik/daten/studie/541806/umfrage/umfrage-zum-identitaetsdiebstahl-in-oesterreich/

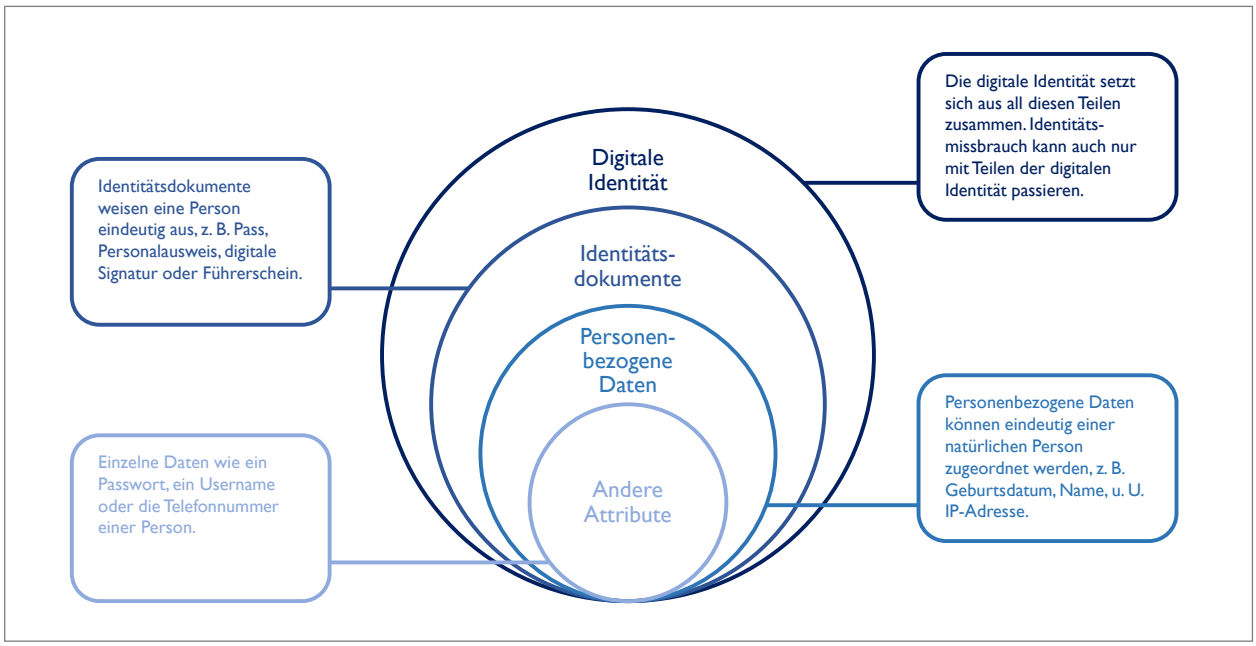

Abb. 1 **Die Zusammensetzung der digitalen Identität.**

1. Identitätsdiebstahl & Identitätsmissbrauch

1.1 Was ist eine digitale Identität?

Durch eine digitale Identität weisen sich Konsument:innen online aus bzw. sie können anhand dieser eindeutig identifiziert werden. Das deutsche Bundeskriminalamt definiert digitale Identität sehr breit als alle Online-Accounts einer Person. Insofern zählen demnach auch die Zugangsdaten z. B. zu E-Mail- und Messenger-Diensten, zu Online-Banking, zu Webshops, Firmen-Websites, E-Government- oder Cloud-Diensten zu Attributen einer digitalen Identität.[3]

Denn die digitale Identität einer natürlichen Person wird über die Zuweisung von Attributen geformt. Attribute sind (1) Ausweisdokumente, (2) personenbezogene Daten (Geburtsdatum, Name, IP-Adresse) und (3) andere Attribute wie die E-Mail-Adresse, Username und Passwörter.

> Im Internet können wir uns anhand einer digitalen Identität zu erkennen geben und eindeutig identifizieren lassen. Personen werden durch ihre digitale Identität im Internet vertreten.

3 Bundeskriminalamt Deutschland (2019). Bundeslagebild Cybercrime. https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2019.html. und Saferinternet.at (Online). Digitale Identität. Was bedeutet das? FAQ. https://www.saferinternet.at/faq/selbstdarstellung/digitale-identitaet-was-bedeutet-das/

1.2 Welche Daten werden gestohlen?

Identitätsdiebstahl meint genau genommen die missbräuchliche Verwendung von Daten einer anderen Person – die Begriffe Identitätsmissbrauch und Identitätsdiebstahl werden im Folgenden synonym verwendet.[4] Zum Teil werden einzelne Attribute einer fremden Identität für die Begehung von Straftaten missbraucht. Kriminelle nutzen auch Daten wie eine Wohnadresse für missbräuchliche Bestellungen oder eine Ausweiskopie für die illegitime Eröffnung von Bankkonten.

Gestohlen und missbräuchlich verwendet werden können viele Daten. Von Zugangsdaten zu diversen Onlinekonten wie dem E-Mail-Account, Online Banking, Social Media, oder auch FinanzOnline oder ELGA, es können eine Vielzahl von Usernamen und Passwörtern betroffen sein.

Auch persönliche Daten und Informationen sind bei Identitätsdiebstahl betroffen. Das umfasst Attribute wie die persönliche Wohnadresse, die Sozialversicherungsnummer, den Arbeitsort oder den:die Arbeitgeber:in, die Telefonnummer, aber auch Informationen zum Privatleben. Hier kann es sich um Fotos und Videos handeln, aber auch um Freundeslisten auf Social Media, oder bestimmte Interessen und Vorlieben, die ausgespäht wurden.

Besonders weitreichende Folgen kann der Missbrauch von Finanzdaten wie Kontoinformationen oder Kreditkartendaten haben. Ebenso die missbräuchliche Verwendung von diversen Urkunden und Ausweisen wie Pass, Personalausweis, E-Card, Führerschein, Impfpass, Grüner Pass oder einer Todesanzeige.

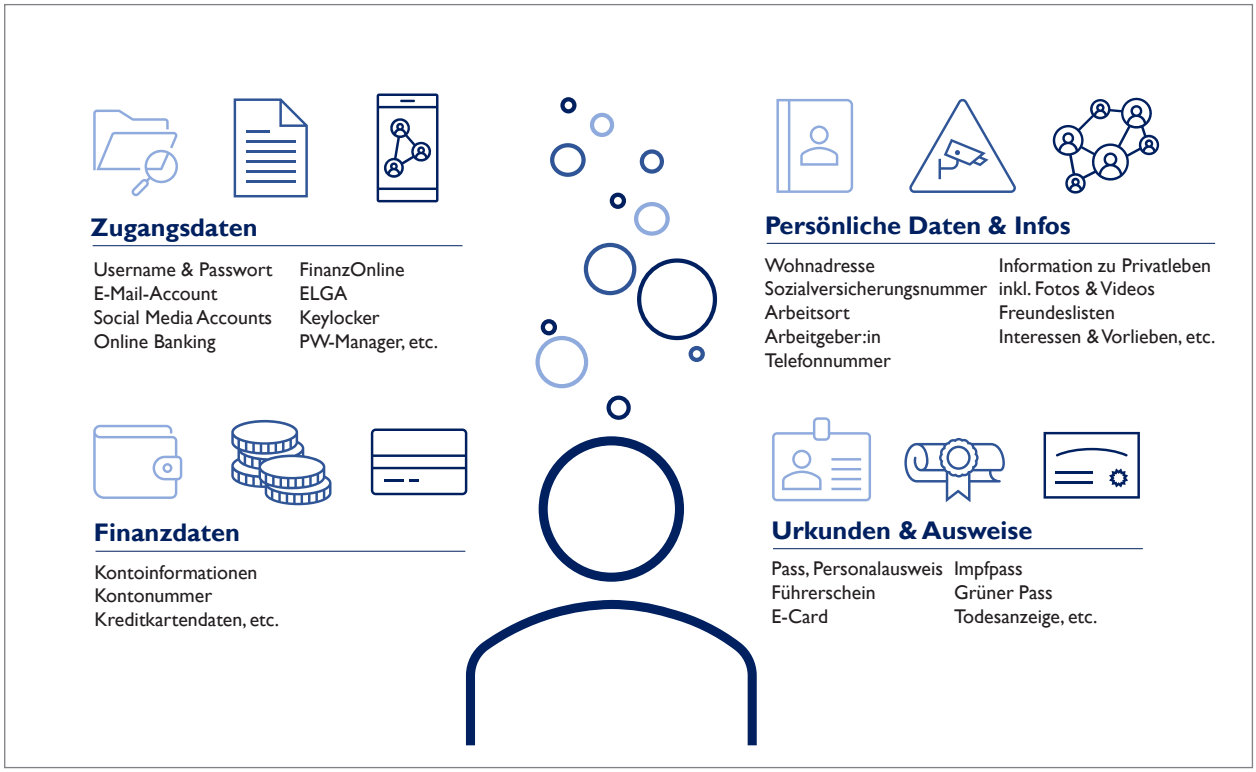

Abb. 2 **Welche Daten für Identitätsmissbrauch gestohlen werden.**

4 Reisch, Lucia A., Bietz, Sabine & Micklitz, Hans-W. (2020). Algorithmen und Verbraucher. Eine Studie im Auftrag des Ministeriums für Ländlichen Raum und Verbraucherschutz (MLR) Baden-Württemberg, Stuttgart. Friedrichshafen: Forschungszentrum Verbraucher, Markt und Politik | CCMP (Hrsg.).

2. Wie gelangen Kriminelle an fremde Daten?

Seit Jahren kommt es in Österreich zu vermehrten Cyberkriminalitäts-Anzeigen. Auch im Jahr 2020 gab es laut Bundeskriminalamt einen Anstieg an diesen Delikten im Vergleich zum Vorjahr um 26,3%.[5] Datendiebstahl ist dabei an vorderster Stelle der begangenen Straftaten, wie eine Studie des Kuratorium Sicheres Österreich zeigt: Jedes vierte Unternehmen war in den vergangenen Jahren von Datendiebstahl betroffen, jedes zehnte wurde von Hackern erpresst.[6] Datendiebstahl betrifft Konsument:innen, unabhängig davon ob sie online aktiv sind.

Kriminelle gelangen an Daten, weil sie öffentlich einsehbar sind (z. B. Online-Telefonbücher), bzw. nutzen sie Eintrittsvektoren, um sich Zugang zu Online-Konten oder persönlichen Daten zu verschaffen: Mit Spam- oder Phishing-Mails, SMS, Fake-Websites oder durch Missbrauch des Remote-Desktop-Protokolls (RDP) erlangen sie die Kontrolle über das fremde IT-System.[7] Durch Täuschung oder den gezielten Einsatz von Tools wie Malware werden Daten wie Passwörter oder Finanzdaten gestohlen.

Das Remote-Desktop-Protokoll (RDP) ist ein Netzwerkprotokoll, das den Fernzugriff auf einen anderen Computer ermöglicht.

Mithilfe des RDP können alle Dateien auf einem Computer gelesen und verändert werden – Kriminelle nutzen diese Anwendung aus, um Opfer und deren Daten auszuspionieren.

Die Kriminellen übermitteln die gestohlenen Daten an externe Instanzen und verwenden diese missbräuchlich. (Kapitel 2.1.) In manchen Fällen kommt es auch zu einer Weiterleitung der Daten ohne den Einsatz von Tools, durch Phishing (Kapitel 2.2.), Fake-Shops (Kapitel 2.3.) oder die Übermittlung von Ausweiskopien im Rahmen von Klein- und Immobilienanzeigen (Kapitel 2.4.) und betrügerischen Jobangeboten (Kapitel 2.5.).

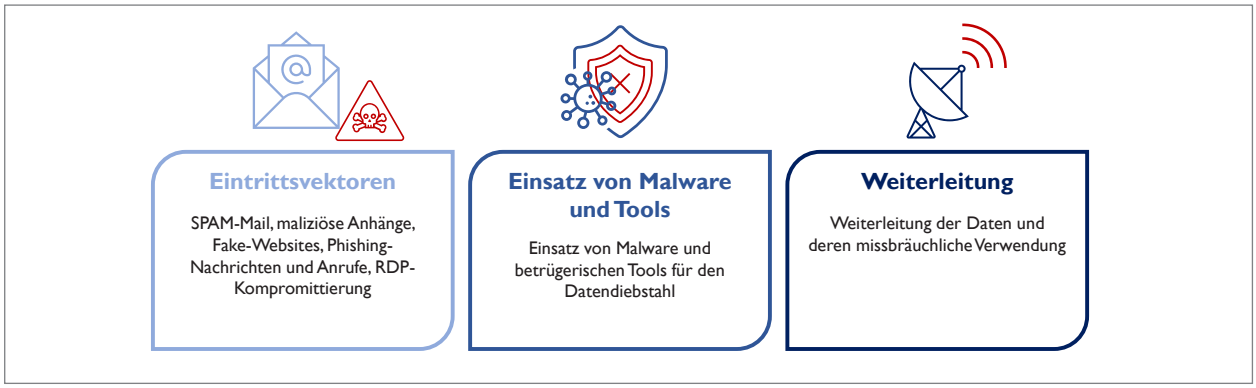

Abb. 3 **Wie gelangen Kriminelle an fremde Daten? Die Daten gelangen über Diebstahl oder Weiterleitung nach außen.**

5 BKA (2021). Cybercrime 2020. https://bundeskriminalamt.at/306/files/Cybecrime_2020_web.pdf
6 ORF.at (2021). Cyberangriffe und Datendiebstahl nehmen „dramatisch" zu. https://orf.at/stories/3210927/
7 Bundeslagebild Cybercrime (2020). https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html

2.1 Datendiebstähle im großen Stil

Datendiebstähle im großen Stil nehmen seit Jahren zu. Der BKA-Bericht zu Cyberkriminalität aus dem Jahr 2020 weist auf die Vorfälle bei österreichischen Unternehmen und Lösegeldforderungen hin. Als Folge dessen hätten die widerrechtlichen Zugriffe auf User-Accounts zugenommen.[8]

Konsument:innen sind vor allem betroffen, wenn große Datensätze von E-Mail-Anbietern oder Social Media-Plattformen gestohlen werden. Im April 2021 betraf es etwa die Daten von 533 Millionen Facebook-Usern inkl. Telefonnummern, Namen, Adressen, E-Mail.[9] Im Mai 2021 wurden die Daten von über 100 Millionen Android-Usern aufgrund von falschen Konfigurationen von Cloud Services von Dritt-Anbietern veröffentlicht.[10] Im Juni waren 7.000 Millionen LinkedIn-User von einer Veröffentlichung eines Datensatzes betroffen.[11]

In der Praxis lässt sich im Nachhinein manchmal nicht klarstellen, ob die Daten von Mitarbeiter:innen nach außen gespielt oder über Angriffe von außen gestohlen wurden. Streng genommen wird jedoch zwischen einem „Data Leak" und einem „Data Breach" unterschieden.

Data Leak

Bei Data Leaks handelt es sich um die nicht autorisierte Übertragung von Unternehmensdaten nach außen. Dies wäre z. B. der Fall, wenn Angestellte die Daten illegal an Externe verkaufen, oder wenn Kriminelle auf Sicherheitslücken stoßen und diese zum Zweck des Datendiebstahls ausnutzen.[12]

Data Breach

Teilweise müssen Kriminelle komplexe Sicherheitsmaßnahmen umgehen oder sich Zutritt durch den Einsatz von Schadsoftware verschaffen – diese Angriffe werden als „Data Breach" bezeichnet. Die gestohlenen Datensätze werden häufig veröffentlicht oder im Dark Net verkauft.

2.2 Phishing

Phishing leitet sich von „password harvesting" und „fishing" (engl.) ab – es bezeichnet das „Fischen nach Passwörtern". Durch gefälschte Websites, E-Mails, Messenger-Nachrichten oder Anrufen versuchen Kriminelle an persönliche oder geheime Daten zu gelangen. Das Ziel ist es Personen zu manipulieren, sodass sie gegen ihre eigenen Interessen handeln. Nachdem diese ihre Zugangsdaten preisgegeben oder Schadsoftware heruntergeladen haben, veranlassen Kriminelle ausgehend davon illegale Zahlungen oder kaufen auf Kosten der Betroffenen ein.

Phishing-Versuche unterscheiden sich nach dem verwendeten Medium, aber auch in der Intensität und dem betriebenen Aufwand, um an bestimmte Daten zu kommen. Es gibt zum einen massenhaft ausgesandte Phishing-Nachrichten, die darauf abzielen durch einen großen Adressatenkreis viele Opfer zu finden. Zum anderen gibt es auch hochgradig individualisierte Phishing-Versuche, z. B. „Spear-Phishing", durch die über eine bestimmte Person Zugang zu einer bestimmten Datenbank eines Unternehmens erlangt werden soll.

Betrügerische Phishing-Nachrichten nutzen z. B. vertraute Firmenlogos und Redewendungen sowie Links zu täuschend echt aussehenden, gefälschten Websites. Oft enthalten Phishing-Nachrichten auch gefährliche E-Mail-Anhänge – nach ihrem Öffnen installiert sich eine Schadsoftware auf dem Computer, Tablet oder Smartphone, die Passwörter und andere Daten ausspioniert. Eine andere Taktik ist es, Personen zur Installation von gefälschten Banking-

8 BKA (2021). Cybercrime Report 2020. S. 10. https://bundeskriminalamt.at/306/start.aspx
9 Holmes, Aron (2021). 533 million Facebook users' phone numbers and personal data have been leaked online. https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4/
10 CheckPoint (2021). Misconfiguration of third-party cloud services exposed data of over 100 million users. https://blog.checkpoint.com/2021/05/20/misconfiguration-of-third-party-cloud-services-exposed-data-of-over-100-million-users/
11 Fortune (2021). Linkedin Data Theft of 700 million users. https://fortune.com/2021/06/30/linkedin-data-theft-700-million-users-personal-information-cybersecurity/
12 F-Secure (2020). Data breach and data leak. https://blog.f-secure.com/data-breach-and-data-leak-whats-the-difference/

Apps oder Schadsoftware zu drängen, die dann ausgeweitete Berechtigungen auf dem infizierten Gerät haben.
Phishing nimmt kontinuierlich zu und nutzt die folgenden Kanäle:

SMS

Seit 2020 häufen sich die User-Meldungen zu Phishing-Versuchen über SMS-Nachrichten bei der Informationsplattform zu Internetbetrug ↗Watchlist Internet.[13] Die Fallen vor denen derzeit wiederholt gewarnt wird, sind: gefälschte Nachrichten von Banken, Paketzustellern oder auch der Polizei.[14] Kriminelle nutzen die SMS, um Konsument:innen dazu zu bewegen, betrügerische Apps herunterzuladen, Bankdaten in gefälschte Masken einzugeben oder Überweisungen zu tätigen. Da SMS zur Zwei-Faktor-Authentifizierung auch von Behörden genutzt werden, ist die Hemmschwelle bei Konsument:innen oft niedriger.

E-Mail

Wenngleich manch Phishing-E-Mail, gespickt mit Tippfehlern, einfach als solches identifizierbar ist, sind die Betrugsversuche inzwischen raffinierter geworden. Ein solcher Fall war ein E-Mail im Jahr 2020, das vorgab von FinanzOnline zu sein. Tausende Konsument:innen in Österreich erhielten das Mail, das Steuerrückerstattungen von tausenden Euro versprach. Wer dem Link folgte, wurde auf eine Website geleitet und zur Eingabe von persönlichen Daten und Kreditkarteninformation aufgefordert.[15] In ähnlicher Weise raffinierte Phishing-Nachrichten waren auch im Namen von Banken und Paketzustellern im Umlauf.

Messenger-Dienste

WhatsApp, Telegram, der Facebook-Messenger, der Instagram-Chat und andere Online-Dienste werden zunehmend als primäres Kommunikationsmittel verwendet. Mit ihrer Popularität steigen auch die Betrugsversuche über diese Dienste. Kriminelle versuchen teilweise über die Initiierung von Dialogen das Vertrauen zum Opfer aufzubauen, um es zur Preisgabe von Daten zu bewegen. Ebenso versuchen Kriminelle über gefälschte Gewinnspiele oder Umfragen Zugang zu Social Media-Accounts zu erlangen.

Anrufe

Phishing erfolgt auch über Telefonanrufe. Häufig kommt es dabei zu angeblichen Anrufen von Bankangestellten, die dazu auffordern Bankdaten herauszugeben oder Überweisungen zu tätigen. Kriminelle geben auch vor für eine IT-Firma, häufig Microsoft, anzurufen. Ihre Masche: Die Person müsse vor Schadsoftware geschützt werden, die angeblich auf deren Computer installiert wurde und ein Programm installieren. Die Kriminellen erlangen jedoch erst eben dadurch die Kontrolle über das Gerät der Betroffenen. Sie können durch die Mithilfe der getäuschten Konsument:innen deren Passwörter und andere Daten ausspähen.

2.3 Fake-Shops

Betrügerische Onlineshops sind für Konsument:innen nicht nur eine Gefahr beim Einkaufen selbst, sondern werden auch für Datendiebstahl genutzt. Über die Bestellformulare werden die Adresse und Kreditkarten-Daten der Betroffenen abgegriffen. Übermitteln Konsument:innen auf diesem Weg ihre Daten, bleibt wenig Spielraum abseits einer Sperre ihrer Kreditkarte und einer polizeilichen Anzeige.

2.4 Kleinanzeigen & Immobilienanzeigen

Eine der „Watchlist Internet" häufig gemeldete Betrugsform läuft über Klein- und Immobilienanzeigen. Meist handelt es sich um Vorschussbetrug: Kriminelle drängen auf eine Geldüberweisung vorab. Auf diesem Weg versuchen sie auch, an persönliche Daten und vor allem Ausweiskopien zu kommen. Interessiert sich jemand z. B. für ein Wohnungsinse-

13 Watchlist Internet. www.watchlist-internet.at
14 Watchlist Internet (2021). Online: https://www.watchlist-internet.at/phishing-datendiebstahl/
15 BKA (2021). Cybercrime Report 2020. S. 14.

rat, verlangen die Kriminellen vor der Vereinbarung eines Besichtigungstermins nach einer „Sicherheit" in Form einer digitalen Pass- oder Ausweiskopie. Wird eine Ausweiskopie übermittelt, wird diese in weiterer Folge kriminell verwendet. Gestohlene Ausweisdokumente werden z. B. als Vertrauensbeweise genutzt, um andere in die Falle zu locken. In der Praxis führt deshalb eine Anzeige von Kleinanzeigenbetrug nicht zu den Kriminellen selbst, sondern zu anderen Betroffenen von Identitätsdiebstahl.

2.5 Betrügerische Jobangebote

Der Nebenjobbetrug und Anzeigen von betrügerischen Marktforschungsinstituten stellen komplexe Betrugsmaschen dar, die sogar strafrechtliche Folgen für die Opfer haben können.[16]

Nebenjobbetrug

Über Medien und Kleinanzeigenplattformen werden betrügerische Stellenausschreibungen verbreitet. Die Kriminellen gaukeln einen Bewerbungsprozess vor und locken im Zuge dessen persönliche Daten sowie Ausweiskopien heraus. Statt eines Jobs erhalten die Betroffenen jedoch erpresserische Nachrichten von ihren angeblichen Chefs: Sie verlangen Geldüberweisungen oder den Kauf von Amazon-Gutscheinen im Wert von mehreren hundert Euro. Kommen die Betroffenen diesen Forderungen nicht nach, wird ihnen mit der Veröffentlichung bzw. dem Verkauf ihrer Daten gedroht.[17]

Betrügerische Marktfoschungsinstitute

Stellenausschreibungen werden auch über betrügerische Marktforschungsinstitute und Umfrageplattformen für Identitätsdiebstahl genutzt. Kriminelle gaukeln vor im Qualitätsmanagement zu arbeiten und Tester:innen zu suchen.[18] Die Bewerber:innen müssen als erste Aufgabe testen, wie der Authentifizierungsprozess bei Onlinebanken vonstattengeht. Was sie nicht wissen ist, dass sie im Zuge dessen tatsächlich ein Konto in ihrem Namen eröffnen und dieses in dem vorgespielten Test authentifizieren. Die Betroffenen haben während des gesamten Prozesses weder Kenntnis über die Existenz des Kontos noch Zugang zu diesem. In weiterer Folge werden kriminelle Tätigkeiten mit dem Konto ausgeführt wie Betrug oder Geldwäsche. Oft erfahren Betroffene erst von dem Betrug, wenn der Polizei ein mit dem Konto in Verbindung stehendes Delikt gemeldet wird.[19]

16 Watchlist Internet (02.12.2020). Betrügerische Jobangebote. https://www.watchlist-internet.at/news/zahlreiche-betruegerische-jobangebote-von-rareai-und-enixai-online/
17 Watchlist Internet (27.11.2017). Stellenausschreibung führt zu Identitätsdiebstahl. https://www.watchlist-internet.at/news/detail/News/stellenausschreibung-als-weihnachtshilfskraft-fuehrt-zu-identitaetsdiebstahl/
18 Onlinesicherheit.gv.at (23.08.2021). Identitätsdiebstahl: Das sind die gängigsten Betrugsmaschen. Online: https://www.onlinesicherheit.gv.at/Services/News/Identit%C3%A4tsdiebstahl--Das-sind-die-g%C3%A4ngigsten-Betrugsmaschen.html
19 Watchlist Internet (23.04.2020). Verhalten Sie sich als würden Sie ein echtes Bankkonto eröffnen. https://www.watchlist-internet.at/news/detail/News/verhalten-sie-sich-als-wuerden-sie-ein-echtes-bankkonto-eroeffnen/

3. Wofür werden gestohlene Daten missbraucht?

Gestohlene Daten werden für unterschiedliche kriminelle Aktivitäten genutzt. Diese reichen von Betrugsmaschen, bei denen Kriminelle vorgeben in einer Notlage zu sein, über den Kauf von Drogen und anderen illegalen Produkten, bis hin zur Unterstützung terroristischer Netzwerke. Schon mit dem Namen, Geburtsdatum und der Adresse einer Person können Kriminelle in fremdem Namen Bestellungen aufgeben und die Produkte an abweichende Lieferadressen schicken lassen. Die Betroffenen erhalten nur die Rechnung oder sogar Forderungen eines Inkassobüros, aber keine Leistung. Es werden auch Mobilfunkverträge mit gestohlenen Identitäten abgeschlossen oder Bankkonten eröffnet, die dann zur Geldwäsche verwendet werden. Im Folgenden ein Überblick über die möglichen Folgen dieser kriminellen Aktivitäten für die Betroffenen von Identitätsdiebstahl.

3.1 Bestell- und Verkaufsbetrug

Zahlreiche missbräuchliche Verwendungen von digitalen Identitätsdaten stehen im Zusammenhang mit Ein- oder Verkäufen im Internet. Auch das Betreiben von Fake-Shops wird durch gestohlene Identitätsdaten ermöglicht. Hier werden die gestohlenen Identitätsdaten von Betroffenen als Impressumsangaben von Fake-Shops verwendet.

Bestellbetrug

Bezeichnet die Bestellung von Produkten und Dienstleistungen mit gestohlenen Daten. Dazu gehört das Bestellen von Produkten auf Rechnung – hierbei bestellen Kriminelle in fremdem Namen diverse Produkte. Die Ware lassen sie nicht an die Adresse der Betroffenen, sondern an eine Abholstation oder zum Standort von Komplizen liefern. Die Opfer erfahren oft erst über die Mahnschreiben der Unternehmen zu ausstehenden Rechnungsbeträgen vom Betrug.

Gestohlene Identitätsdaten werden auch für den Abschluss von Mobilfunkverträgen missbräuchlich verwendet.[20] In Österreich ist es nur mit einer Passkopie möglich einen Prepaid-Mobilfunkvertrag abzuschließen. Dieser Vertrag kann dann in einen laufenden Vertrag auf Rechnung, ohne zusätzliche Identitätsüberprüfung umgewandelt werden. Betroffene erhalten in Folge Mobilfunkrechnungen, ohne dass sie über den Vertrag Bescheid wissen.

Wurden Kreditkartendaten gestohlen, macht sich der Betrug nur durch unautorisierte Abbuchungen am Konto der Betroffenen bemerkbar. Da Kreditkartenabrechnungen erst am Ende des Monats passieren, kann enormer finanzieller Schaden entstehen, bis der Betrug entdeckt und die Karte gesperrt wird. Kriminelle erwerben z. B. Hörbücher oder Software im fremden Namen und verkaufen die erworbenen Lizenzschlüssel weiter. Sie schließen auch Abos für kostenpflichtige Streaming-Dienste, Online-Dating-Portale oder Premium-E-Mail-Accounts ab. Dafür werden auch Online-Konten gehackt, auf denen Zahlungsinformationen hinterlegt sind.

Verkaufsbetrug

Liegt vor, wenn Kriminelle gestohlene Daten in Form von Marktplatzkonten missbrauchen. Sie übernehmen die Konten von legitimen Verkäufer:innen und schließen Verträge mit Konsument:innen ab. Diese bezahlen die Produkte, erhalten die Waren jedoch nie. Laut eBay sind Useranfragen zu unerwünschten Accountübernahmen im Jahr 2021 um 250% gestiegen, Kontosperrungen auf der Plattform

20 Verbraucherzentrale.de (2021). Welche Folgen Identitätsdiebstahl im Internet haben kann. https://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/welche-folgen-identitaetsdiebstahl-im-internet-haben-kann-17750

stiegen um 200%. Mittlerweile machen Support-Anfragen zu diesem Thema die Hälfte aller Anfragen aus.[21]

3.2 Geldwäsche

Eine schwerwiegende Folge von Identitätsdiebstahl ist, wenn Bankkonten im Namen der Betroffenen eröffnet werden. Diese Konten werden dann für illegale Aktivitäten wie Betrug (d. h. als Empfängerkonto für Zahlungen von betrogenen Personen) oder Geldwäsche missbraucht. Da das Konto unter dem Namen des Betroffenen des Identitätsdiebstahls geführt wird, geraten zunächst einmal die betroffenen Personen ins Visier der Strafverfolgungsbehörden. Mangels Vorsatzes wird in den seltensten Fällen eine strafrechtliche Verantwortung vorliegen.

In Frage kommt allerdings eine mögliche schadenersatzrechtliche Haftung als Nebentäter, wenn den Betroffenen des Identitätsdiebstahls ein fahrlässiges Verhalten vorwerfbar ist. Sofern die von Identitätsdiebstahl betroffenen Personen nämlich durch ein eigenes schuldhaftes (fahrlässiges) Handeln einen Beitrag zur Schädigung der Betrugsopfer geleistet haben, kann eine zivilrechtliche Mithaftung mit den eigentlichen Betrügern gegenüber dem Betrugsopfern nicht ausgeschlossen werden.

2021 hat die deutsche Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) Maßnahmen angeordnet, die die Onlinebank N26 verpflichten eine ordnungsgemäße Geschäftsorganisation sicherzustellen und Risiken einzudämmen.[22] Diese Maßnahmen sind eine Folge zahlreicher illegitimer Bankkonten, die in Verdacht stehen für Geldwäsche und Terrorismusfinanzierung missbraucht worden zu sein.[23] Zusätzlich wurde der Bank eine Geldstrafe von 4,25 Millionen Euro auferlegt sowie eine Beschränkung von maximal 50.000 Konto-Neueröffnungen pro Monat.

3.3. Missbrauch von Onlinekonten & Erstellung von Fake-Profilen

Gestohlene Identitätsdaten werden auch zur missbräuchlichen Verwendung von Onlinekonten und der Erstellung von Fake-Profilen verwendet, mit ärgerlichen Folgen für Betroffene und deren Kontakte.

SPAM-Nachrichten

Problematisch sind bei gestohlenen Zugangsdaten für Social Media-Konten unter anderem mögliche Schneeballeffekte. So passiert z. B. auf der Plattform Instagram: Ein User bekam eine Direktnachricht von einer befreundeten Person, mit der Aufforderung an einem Gewinnspiel teilzunehmen. Die einzige Bedingung war es, auf einen Link zu klicken und die eigenen Instagram-Login-Daten preiszugeben. Der User kam der Aufforderung nach, nur um einige Momente später, aus dem eigenen Account ausgesperrt zu werden – Kriminelle hatten über die Gewinnspiel-Maske, die Zugangsdaten des Users erhalten und so den Account gekapert. In Folge wurden dann Nachrichten von dem gekaperten Account aus verschickt, um weitere Personen in die Falle zu locken.

Dieser Vorfall illustriert ein häufiges Problem: Über das Aussperren der User von ihren Social Media-Accounts können Kriminelle massenweise Spam-Nachrichten an die Kontakte der Opfer senden. Diese Nachrichten sind weitere Versuche von Identitätsdiebstahl. Sie enthalten z. B. Links zu Websites, auf denen User ihre Account-Daten in Phishing-Masken eingeben sollen. Da diese Nachrichten von bekannten und vertrauenswürdigen Accounts versendet werden, fallen User eher auf den Betrug herein. Hier wird der Effekt der sozialen Nähe auf Social Media ausgenutzt, um massenweise Zugangsdaten zu Accounts zu stehlen.

21 Chip.de (2021). Gefahr bei eBay Kleinanzeigen: Kriminelle übernehmen Nutzer-Accounts – so schützen Sie sich. https://www.chip.de/news/eBay-Kleinanzeigen-Gefahr-durch-Account-Uebernahmen_183976113.html

22 Bundesanstalt für Finanzdienstleistungsaufsicht (2021). N26 Bank GmbH: BaFin ordnet Wachstumsbeschränkung an und bestellt Son-derbeauftragten. https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Massnahmen/60b_KWG_84_WpIG_und_57_GwG/meldung_211109_60b_N26.html

23 Handelsblatt (2021). Betrüger könnten mehr als 1000 Konten von N26 genutzt haben. https://www.handelsblatt.com/finanzen/banken-versicherungen/banken/geldwaesche-betrueger-koennten-mehr-als-1000-konten-von-n26-genutzt-haben/27522976.html

Gestohlene Influencer:innen-Accounts

Übernehmen Kriminelle den Account von Influencer:innen, kann das massive Auswirkungen haben. Ist beispielsweise eine Kreditkarte hinterlegt worden, wie es bei Facebook-Diensten möglich ist, können Kriminelle über einen Account Werbeanzeigen schalten, ohne dafür zu zahlen. Auch kleinere Influencer:innen haben tausende Follower. Der finanzielle Schaden ist enorm und der Ruf von Influencer:innen leidet. Wenn über die gestohlenen Accounts massenweise Spam oder betrügerische Werbeanzeigen geschaltet werden, hat dies Folgen für tausende Konsument:innen. Teilweise wird die Übernahme von Influencer:innen-Accounts für „Social Extortion" genutzt – Kriminelle verlangen Geld für die Rückgabe des Accounts.

Mobbing & Stalking

Es kommt auch zu Identitätsdiebstahl in Gewaltverhältnissen durch (Ex-)Partner:innen oder im Rahmen von Stalking. In diesen Fällen geht es bei dem Identitätsdiebstahl weniger darum den Betroffenen finanziell zu schaden, sondern die Person enormer psychischer Belastung auszusetzen und ihren Ruf zu ruinieren. Die Täter:innen haben durch persönliche Verbindung möglicherweise Kenntnis von den Passwörtern der Betroffenen. Sie nützen dies aus, um Social Media-Konten zu übernehmen oder erstellen Fake-Accounts mit Daten und Bildern der Person. Strafdelikte, die in Zusammenhang mit diesen Arten des Identitätsdiebstahls stehen sind z. B. die unautorisierte Veröffentlichung von Nacktfotos.

4. Welche Folgen hat Identitäts-missbrauch?

Betroffene von Identitätsmissbrauch können mit finanziell schwerwiegenden, vor allem aber mit langwierigen Konsequenzen zu kämpfen haben. Sind Konsument:innen einmal zum Opfer geworden, dauert es in extremen Fällen Jahre, bis sie dem Kreislauf der Folgen wieder entkommen. Die Folgen umfassen:

Finanzielle Schäden

Betroffene haben mit finanziellen Konsequenzen zu kämpfen. Sie erhalten etwa laufend Rechnungen für Bestellungen, von denen sie nichts wussten. Sie sind mit Forderungen von Inkassobüros konfrontiert und auf ihren Kontoauszügen finden sie unautorisierte Abbuchungen. Weil Bestellbetrug in ihrem Namen durchgeführt wurde, verschlechtert sich ihre Bonität und daran geknüpft wird z. B. die Inanspruchnahme von Krediten schwierig. Auf Betroffene kommen gegebenenfalls Anwaltskosten zu, um sich gegen die Anschuldigungen effektiv zu wehren.

Strafrechtlich relevante Problemstellungen

Gestohlene Identitätsdaten werden missbraucht, um Bankkonten zu eröffnen und damit strafrechtlich relevante Taten zu begehen. Das ist den Betroffenen nicht bewusst, solange sie nicht mit den Strafanzeigen konfrontiert sind. Die Betroffenen geraten dann in einen Teufelskreis, aus dem sie nur schwer entkommen: Denn wird ihre Identität zum Begehen von Straftaten missbraucht, bleibt es meist nicht bei einem Vorfall und sie sehen sich wiederholt Beschuldigungen durch Ermittlungsbehörden ausgesetzt, die oft nicht leicht zu entkräften sind.

Persönlichkeitsrechtsverletzungen & Reputationsschäden

Der Missbrauch von gestohlenen Social Media-Accounts, Fotos und persönlichen Daten kann zu Persönlichkeitsrechtsverletzungen und erheblichen Reputationsschäden führen. Das ist z. B. der Fall bei „Revenge Porn", der illegalen Veröffentlichung von pornografischem Material von Expartner:innen.

Zeitlicher Schaden & psychische Belastung

Die Aufklärung und Schadensbehebung nach einem Identitätsdiebstahl können Jahre in Anspruch nehmen. Gehen diese einher mit Reputationsschäden und anderen Folgen, bedeutet das eine außerordentliche psychische Belastung für Betroffene. Oft ist nicht klar, wie sie den Missbrauch überwinden und den künftigen Missbrauch ihrer gestohlenen Identität verhindern können. Wurden die Daten von Betroffenen in einem Data Leak veröffentlicht, sind diese weiterhin offen verfügbar, was zu einem allgemeinen Unsicherheitsgefühl beiträgt.

Eindrucksvoll schildern diese Reportagen die Folgen von Identitätsdiebstahl.

- **Der Fall der Journalistin Tina Groll:** Nur ihren Namen und ihr Geburtsdatum verwendeten Kriminelle, um Bestellbetrug in Höhe von Tausenden Euro zu begehen. Laut Groll, die als Journalistin und Autorin arbeitet, war jedoch nicht der Identitätsmissbrauch selbst, sondern die Folgen die größte Herausforderung: Sie musste über 800 Arbeitsstunden und hohe Anwaltskosten aufbringen, um sich erfolgreich gegen Inkassobüros und Gerichtsurteile zu wehren.[24]

- **Der Fall des Influencers Steven Epprecht:** Der Schweizer Influencer ist durch Identitätsdiebstahl zum Gesicht von Investment-Betrug geworden – er kann bislang nicht erfolgreich dagegen vorgehen, da die Täter:innen nicht zu fassen sind. Der Account der missbräuchlich

24 Tina Groll (2022). Identitätsdiebstahl. https://tina-groll.de/index.php/identitaetsdiebstahl

Epprechts Daten und Fotos verwendet, hat schon mehr als 200.000 Follower und lockt diese in Investmentfallen. In diesem Fall hat Identitätsmissbrauch nicht nur negative Auswirkungen auf Epprecht als Betroffenen, sondern auch auf tausende Konsument:innen, die durch das vertrauenswürdig wirkende Fake-Profil getäuscht werden.[25]

- **Reportage zu Identitätsmissbrauch durch Ex-Partner:** Die Daten und Fotos einer Frau werden von ihrem Ex-Partner auf Social Media und auf Dating-Profilen missbräuchlich verwendet. Er benutzt diese, um sie selbst aber auch andere zu bedrohen und zu belästigen. Eine Anzeige erstatten will die junge Frau nicht, da der des Stalkings verdächtigte Täter dadurch mittels Akteneinsicht Zugriff auf ihre Adresse erlangen könnte. Diese Reportage kritisiert die fehlende Aufklärung von Polizei und den fehlenden Opferschutz in persönlichen Fällen von Identitätsdiebstahl bei denen der Täter bekannt ist.[26]

25 20min.ch (2021). Russischer Dieb klaut Online-Identität von Influencer Steven Epprecht. https://www.20min.ch/story/russicher-dieb-klaut-online-identitaet-von-influencer-steven-epprecht-252547368477
26 20min.ch (2021) ibid.

5. Handlungsansätze und Maßnahmen

Um Identitätsdiebstahl zu bekämpfen, sind Maßnahmen mit unterschiedlichen Ansätzen erforderlich: Einerseits geht es um die Schaffung einer sicheren Ausgangslage, andererseits stehen für Betroffene Schadensbegrenzung und Unterstützungsangebote im Mittelpunkt. Die Maßnahmen zur Minimierung der Risiken rund um Identitätsdiebstahl stehen jedoch immer auch in einem Spannungsfeld mit dem Schutz der Privatsphäre bzw. dem Recht auf Anonymität.

In den vergangenen Jahren ist der Druck für Verbraucher:innen, sich elektronisch auszuweisen, gestiegen. Teilweise werden Identitätsverifizierungen als Maßnahme gegen Betrug und Missbrauch angesehen, z. B. wenn Vermieter:innen auf die Online-Übermittlung von Ausweiskopien drängen, um sich abzusichern. Teilweise finden Identitätsverifikationen verstärkt als Konsequenz gesetzlicher Regelungen statt, z. B. im Rahmen von Altersverifikationen.

Das Spannungsfeld zwischen dem Recht auf Anonymität und Sicherheitsmaßnahmen offenbart sich in der aktuellen Debatte zur elektronischen Ausweispflicht. Denn die Übermittlung von Daten, um die eigene Identität zu verifizieren, kann auch ein Risiko für Konsument:innen darstellen. Die Sicherheitsversprechen von Biometrie werden z. B. von Expert:innen der Österreichischen Akademie der Wissenschaften als überzogen bewertet.[27]

5.1 Die Schaffung einer sicheren Ausgangslage

Um die Daten von Konsument:innen zu schützen, braucht es zahlreiche Maßnahmen an neuralgischen Punkten. Technische Vorgehensweisen reichen von der digitalen Identifizierung, über die Zwei-Faktor-Authentifizierung hin zur sicheren Übermittlung und Speicherung der Daten durch Unternehmen.

Technische Lösungen allein greifen jedoch zu kurz, wenn es um die Prävention von Identitätsmissbrauch geht. Denn das Wissen von Konsument:innen zu Fallen und der verantwortungsvolle Umgang mit ihren Daten und persönlichen Informationen, sind essenziell für ihre Ermächtigung zum Selbstschutz. In Kapitel 7 finden sich dazu Tipps für Konsument:innen zur Frage „Wie kann ich mich gegen Identitätsmissbrauch schützen?“. Die Herausforderung, die es bei der Vermittlungsarbeit zu bedenken gilt, ist, dass Sicherheitsmaßnahmen einen Aufwand darstellen und oft zulasten von Benutzerfreundlichkeit gehen. Es überrascht folglich nicht, dass Konsument:innen teilweise auf Sicherheitsmaßnahmen verzichten, sei es aus Bequemlichkeit oder mangelndem Wissen.

Es sind jedoch nicht nur die Konsument:innen gefragt, wenn es um die Schaffung einer sicheren Ausgangslage im Sinne der Prävention geht. Plattformen, E-Commerce-Anbieter:innen und letztlich der Staat können viel unternehmen, um Konsument:innen zu schützen. Im Folgenden sind potenzielle Handlungsansätze und Maßnahmen beschrieben.

27 ÖAW (2021). Massenüberwachung durch Biometrie. https://www.oeaw.ac.at/ita/detail/news/massenueberwachung-durch-biometrie

5.1.1 Digitale Identifizierungen

Konsument:innen müssen sich online auf unterschiedliche Weise ausweisen – z. B. verlangt eine Social Media-Plattform den Namen und das Geburtsdatum, das digitale Amt hingegen einen verifizierten Identitätsnachweis. Nicht zuletzt aus diesen unterschiedlichen Anforderungen sich online zu identifizieren, ist eine Landschaft der digitalen Identifizierungssysteme entstanden, mit staatlichen und privatwirtschaftlichen Akteuren.

Das Feld der digitalen Identifizierungen wird massiv von privaten Akteuren bespielt. Die größten Player mit eigenen Lösungen sind Apple und Google. Apple hat ein biometrisches Authentifizierungsverfahren entwickelt und mit der Gesichtserkennungssoftware einen Standard in der Smartphone-Branche geschaffen.[28] Google bietet mit dem „Google Authenticator" eine App-Lösung zur Zwei-Faktor-Authentifizierung an und rät, diesen für alle Google-Dienste zu aktivieren. Die digitalen Identifizierungen von Google und Apple haben sich auch als Identifizierungsmethoden für andere Plattformen etabliert – mit nur wenigen Klicks eröffnen Konsument:innen auf diese Weise neue Accounts. Für sie bequem, die Unternehmen Google and Apple erhalten dadurch Einblick in ihre Interessen.

Parallel zu den privatwirtschaftlichen Lösungen hat die elektronische Identifizierung auch in der digitalen Verwaltung Einzug gehalten.[29] In Österreich konnte ab dem Jahr 2003 die digitale Bürgerkarte mithilfe eines Kartelesegeräts und einer Karte (wie der e-Card) aktiviert werden. Jedoch können seit 2019 keine neuen e-Cards als Bürgerkarten registriert werden und das physische Bürgerkarten-Modell ist zugunsten der Handysignatur im Jahr 2021 ausgelaufen.[30] Derzeit ist neben der möglichen Nutzung der digitalen Bürgerkarte auch die Handysignatur im Einsatz. Diese funktioniert mithilfe eines Mobiltelefons mit SMS-Funktion und wird vom österreichischen Unternehmen „A-Trust" verwaltet.[31] Um Behördenwege online zu erledigen kann derzeit mittels Handysignatur z. B. die App „Digitales Amt" genutzt werden.[32]

ID-Austria

Die neu eingeführte, derzeit und bis Mitte 2022 noch in der Pilotphase befindliche ID-Austria ist eine Weiterentwicklung der Handysignatur und Bürgerkarte.[33] Sie hat alle Funktionen der Handysignatur und umfasst mit der ID-Austria auch die Möglichkeit eines elektronischen Identitätsnachweises – beispielsweise sind Dokumente wie der Führerschein dann digital verfügbar.[34]

Die ID-Austria ist im Kontext der aktuellen Debatte rund um die Einführung einer europaweit zu nutzenden elektronischen Identität zu sehen. Die Europäische Kommission strebt eine Änderung der „eIDAS-Verordnung"[35] im Sinne der Harmonisierung und Weiterentwicklung des Rahmens für eine sichere öffentliche elektronische Identifizierung (E-ID) an. Konsument:innen sollen ihre staatlichen E-IDs nicht nur für Behördenwege, sondern auch für die Nutzung privater Dienste (z. B. Social Media) einsetzen können. Damit soll auch ein Konkurrenzmodel zu privatwirtschaftlichen Identifizierungslösungen geschaffen werden – statt des schnellen Klicks auf die Lösungen von Apple, Google und Co. würde eine öffentliche Lösung genutzt werden können.

Kritik

Der EU-Vorstoß zu einer solchen E-ID Lösung stößt auch auf Kritik. Diese bezieht sich auf die notwendige, aber teils als nicht ausreichend bewerteten Anforderungen an die Sicherheits-Infrastruktur.

28 Hill, Simon (2017, November). Can facial recognition really replace fingerprints? https://www.digitaltrends.com/mobile/is-facial-recognition-the-new-security-standard/
29 BMDW (2022). Digitales Österreich. https://www.bmdw.gv.at/Themen/Digitalisierung/Digitales-Oesterreich.html
30 Die Bürgerkarte. https://www.buergerkarte.at/faq-karte.html
31 Die Handy Signatur. https://www.buergerkarte.at/anwendungen-handy.html
32 Österreich.gv.at (2022). Digitales Amt. https://www.oesterreich.gv.at/app-digitales-amt/faq/allgemein.html
33 Österreich.gv.at (2022). ID Austria. https://www.oesterreich.gv.at/themen/dokumente_und_recht/id-austria/pilotbetrieb.html
34 Iosa, Andreea (2021, August). Nachfolger der Handy-Signatur: Was bringt ID Austria? In: Futurezone.at. https://futurezone.at/digital-life/digitaler-ausweis-id-austria-fuehrerschein-handy-signatur-buergerkarte/401480884
35 Europäische Kommission (2021). Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität. https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A52021PC0281&qid=1644488241088

Auch geht es um die in die E-ID Bereitstellung und die Kontrolle der Identitäten eingebundenen Akteure. Das Konzept einer E-ID im Sinne eines staatlich bereitgestellten elektronischen Identitätsnachweises suggeriert die Handhabung durch öffentliche Akteure, doch es können in die Abwicklung durchaus auch Private als Serviceprovider involviert sein. Kritiker:innen verlangen deshalb eine Evaluierung des öffentlichen und privaten E-ID Infrastrukturkonzepts bzgl. wirtschaftlicher Interessen, Datensicherheit und Privatsphäre.[36]

Die mögliche Nutzung der E-ID für private Zwecke führt zur Sorge, dass dadurch z. B. für soziale Medien eine Ausweispflicht eingeführt würde – eine Gefahr für das Recht auf Anonymität im Netz. Epicenter Works sieht darin „einen billigen Weg, die Kunden zu identifizieren."[37] In der jetzigen Form des Vorschlags könnten alle mit ID-Austria getätigten Transaktionen einer Person nachvollzogen werden, es könnte also verfolgt werden, wo jemand sich digital identifiziert. Demnach könnte eine Nachverfolgung von Konsument:innen über unterschiedliche E-ID-Einsatzgebiete hinweg möglich sein, sofern es nicht wie z. B. beim Modell der digitalen Signatur getrennte Datensilos für Aktionen gibt. Die Sorge: Verwendet jemand den digitalen Impfpass, bzw. Grünen Pass beim Einchecken in ein Hotel, den digitalen Führerschein beim Autoverleih und die E-ID zum Einloggen in FinanzOnline, könnten diese Aktionen auf die E-ID rückschließbar sein.

Kritiker:innen verlangen daher die Entwicklung einer datenschutzkonformen E-ID entlang von Privacy-by-Design Ansätzen. Angelehnt an „Good Practices" wie z. B. der Handysignatur, sollten Konzepte entwickelt werden, die in ihrer Wirksamkeit in Abhängigkeit mit damit zusammenhängenden Risiken durch Datensammlung und Überwachung, sowie dem Recht auf Anonymität, evaluiert werden. Im Gegensatz zur digitalen Bürgerkarte und der Handysignatur, bringt die E-ID Austria mit sich, dass es ein Smartphone braucht und derzeit zusätzlich eines mit biometrischen Authentifizierungsmöglichkeiten, wie ein Fingerabdruckscanner oder der biometrischen Gesichtserkennung. Dies wird kritisiert, dazu kommt auch Bedenken bezüglich möglicher Ungleichbehandlung aufgrund von digital günstigeren Behördenwegen (wegen der geringeren Bearbeitungsgebühr).[38]

5.1.2 Die Zwei-Faktor-Authentifizierung

Die Zwei-Faktor-Authentifizierung hat Einzug in den Alltag von Konsument:innen gefunden. Im Bankwesen wurde sie 2018 verpflichtend für den europäischen Wirtschaftsraum über die EU-Zahlungsdienste-Richtlinie eingeführt. Seither ist es verpflichtend, für den Zugang zu Onlinebanking, zu Banking-Apps, und bei einigen Zahlungen im Internet eine starke Kund:innen-Authentifizierung zu verwenden.

> Die Zwei-Faktor-Authentifizierung (2FA) bezeichnet den Identitätsnachweis einer Person durch zwei unterschiedliche und unabhängige Komponenten (Faktoren).
>
> Die 2FA wird beispielsweise beim Onlinebanking oder bei der Handy-Signatur verpflichtend angewandt.

Plattformen wie Google, Amazon aber auch Facebook-Dienste bieten die Zwei-Faktor-Authentifizierung an, um Accounts besser zu schützen. Bei der 2FA wird meist Wissen (das Passwort) mit einem persönlichen Besitz (Mobiltelefon, Authentifizierungs-App, Sicherheitsschlüssel, etc.) kombiniert. In der Praxis handelt es sich bei dem Faktor Besitz oft um einen Code, der per E-Mail oder SMS verschickt, oder in einer Authentifizierungs-App angezeigt wird.[39] Auch kann der zweite Faktor ein physischer

36 Manakas und Mey (2022). ID Austria: Die wichtigsten Fakten zum digitalen Smartphone-Ausweis. In: Der Standard. https://www.derstandard.at/story/2000134132775/id-austria-die-wichtigsten-fakten-zum-digitalen-smartphone-ausweis

37 Lohninger, Thomas (2021). Orwells Wallet. https://epicenter.works/content/orwells-wallet-das-elektronische-identifizierungssystem-der-eu-fuehrt-uns-direkt-in-den

38 Lohninger, Thomas (2021). ibid.

39 Proschofsky, A. (3.4.2022). Zwei-Faktor-Authentifizierung: Wie es geht und warum der zusätzliche Schutz so wichtig ist. https://www.derstandard.at/story/2000134600410/zwei-faktor-authentifizierung-wie-es-geht-und-warum-der-zusaetzliche

„Schlüssel" in Form eines USB-Sticks sein. Auch Plattformen, wie z. B. Google drängen Konsument:innen dazu, einen zweiten Faktor bei ihrem Konto hinzuzufügen, um die Kontensicherheit aber auch eine mögliche Kontenwiederherstellung zu garantieren. Verpflichtend ist der zweite Faktor jedoch nicht.

Die verpflichtende Verwendung der 2FA auch bei diesen Anbietern könnte Schutz vor Identitätsdiebstahl bieten, würde jedoch die Hürden zum Einstieg in diese Plattformen erhöhen und ist in Abwägung mit den Ansprüchen von Konsument:innen auf Anonymität im Internet wichtig. Zu bemerken ist, dass bei der 2FA privatwirtschaftliche Akteure Standards setzen, die dann in Folge von politischer Seite legitimiert werden. Hier schaffen somit privatwirtschaftliche Akteure, zumeist große Plattformen wie Google Standards für Anwender:innen.

5.1.3 Risiken beim Versand von Ausweiskopien minimieren

Der Versand von Ausweiskopien birgt ein großes Missbrauchspotenzial. In Deutschland bestand deshalb bis 15.07.2017 ein grundsätzliches Verbot, Ausweiskopien zu erstellen [§ 20 Abs 2 Personalausweisgesetz idF vor dem Gesetz vom 07.07.2017 ↗ BGBl. I S. 2310 (Nr. 46)]. Mittlerweile wurde dieses Verbot aufgeweicht – auch weil sich dieses in vielen Anwendungsfällen schwer umsetzen ließ. Aber auch nach aktueller Rechtslage ist die Erstellung von Ausweiskopien nur unter bestimmten Voraussetzungen erlaubt. Außerdem muss in Deutschland zum Schutz vor Missbrauch jede Ausweiskopie als solche gekennzeichnet sein.

In Österreich bestehen hinsichtlich der Anfertigung von Ausweiskopien keine ausdrücklichen Regelungen. Das Erstellen von Ausweiskopien unterliegt aber datenschutzrechtlichen Regeln und kann mit dem Grundsatz der „Datenminimierung" gemäß Art 5 Abs 1 lit c Datenschutz-Grundverordnung unvereinbar sein. Zu überlegen wäre, ob eine Einschränkung der Möglichkeit, Ausweiskopien zu verlangen gesetzlich verankert werden soll bzw. inwiefern ein Versenden von Ausweiskopien nur mit Wasserzeichen zum Standard werden sollte.

Anzudenken wären auch Alternativen zur sicheren Übermittlung von Ausweisen, beispielsweise im Sinne von Upload-Möglichkeiten bei Behörden. Jedenfalls möglich ist es, im Rahmen der Datenminimierung – geschwärzte Ausweiskopien zu übermitteln, die nur Namen und Geburtsdatum preisgeben. Es ist ratsam die restlichen Informationen abzudecken oder zu schwärzen – etwas, das Unternehmen im besten Fall den Konsument:innen auch eindeutig als Hinweis mitteilen sollten. Einem Urteil aus den Niederlanden zufolge ist dies eine Pflicht.[40]

5.1.4 Das Management von Kund:innendaten

Die Speicherung und Verarbeitung von Kund:innendaten durch Unternehmen stellen ein Risiko für Konsument:innen dar. Um die Sicherheit der Kund:innendaten zu gewährleisten, muss zum einen die Sicherheit der Infrastruktur bestehen – also eine Systemsicherheit. Es sollten Encryption und Privacy-Ansätze zum Tragen kommen. Zum anderen sollten auch Sicherungskopien und Zugänge zu diesen sensiblen Daten verantwortungsvoll gehandhabt werden. Mitarbeitende müssen hierfür gut geschult sein. Über die Anwendung von Leak-Checkern und dem Abgleich mit Datenbanken können Unternehmen sicherstellen, dass kein Data Leak stattgefunden hat. Zudem ist zu gewährleisten, dass Konsument:innen im Falle des Falles rasch kontaktiert werden. (Siehe Kapitel 5.1.)

5.1.5 Die Detektion von Betrugsmustern

Unternehmen versuchen über die frühzeitige Erkennung von Betrugsmustern User und sich selbst vor Missbrauch zu schützen. Dafür wird auch Künstliche Intelligenz eingesetzt, zum Beispiel für die Fernidentifikation von natürlichen Personen und Geräten. Um sicherzustellen, dass es sich bei der angenommenen Person tatsächlich um diese handelt, werden bildverarbeitende Ansätze sowie automatisierte Authentifizierungsverfahren einge-

40 European Data Protection Board (2022, März). Dutch SA fines DPG Media Magazines for unnecessarily requesting copies of identity documents. https://edpb.europa.eu/news/national-news/2022/dutch-sa-fines-dpg-media-magazines-unnecessarily-requesting-copies-identity_en

setzt. Ähnliche Verfahren werden auch zur eindeutigen Erkennung von persönlichen Geräten eingesetzt, um ein Gerät (Smartphone oder Computer) klar zu identifizieren.

Es kommen Lösungen zum Einsatz, die einen Datenabgleich mit gepoolten Daten und großen Datenbanken machen. Hierbei werden Informationen, die beispielsweise im Rahmen einer Bestellung erhoben werden, mit Daten in Datenpools abgeglichen und vernetzt. Unter Anwendung von Mustererkennung wird nach Verbindungen zu bekannten Betrugsfällen gesucht. Zusätzlich ermöglichen Lösungsanbieter auch einen gezielten Informationsservice über Betrugsfälle und versuchte Fälle von Betrug.[41]

Durch den Einsatz von „Behavioral Biometrics", der Analyse von menschlichem Verhalten durch automatisierte Systeme versuchen Unternehmen Betrugsmuster, auffällige Transaktionen oder die betrügerische Erstellung von falschen Kundenkonten zu erkennen und zu unterbinden. Momentan gibt es keine Stelle, außer der Datenschutzbehörde, die sich mit dem Missmanagement von Kund:innendaten beschäftigt. Oftmals ist es schwierig für Konsument:innen, überhaupt von Data Leaks oder Schwachstellen im Datenmanagement zu erfahren.

5.2 Maßnahmen nach Identitätsdiebstahl & Schadensbegrenzung

Wenn Betroffene realisieren, dass sie von Identitätsdiebstahl betroffen sind, stehen sie vor der Frage: Was ist zu tun? Es zeigt sich dabei, dass ein Entkommen aus der Spirale des Identitätsdiebstahls schwierig, zeit- und kostenintensiv sein kann. Im Folgenden werden bereits existierende oder angedachte Maßnahmen im Schadensfall näher erläutert.

5.2.1 Leak Checker & Monitoring-Tools

Es gibt eine Reihe an Tools zur frühzeitigen Erkennung von Identitätsdiebstahl, die vor allem von Unternehmen genutzt werden sollten – auch um ihre Kund:innen selbst frühzeitig zu warnen. Konsument:innen könnten diese ebenfalls einsetzen, um frühzeitig auf Data Leaks aufmerksam zu werden.

Hinweise auf Leaks von Unternehmensseite

Banken aber auch Social Media-Plattformen müssen laut DSGVO (Art. 33, 34) ihre Kund:innen darauf hinweisen, wenn sich ein hohes Risiko aus einem Data Leak ergibt. Ebenso sind alle Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde zu melden. Hier ist Verbesserungspotenzial zu sehen, denn die Benachrichtigungen erreichen Konsument:innen oft erst einige Monate oder sogar Jahre nach dem eigentlichen Data Leak.

Passwortmanager & Screening

Passwortmanager weisen Konsument:innen darauf hin, wenn das eigene Konto von einer Sicherheitslücke betroffen ist. Sie bieten auch automatische Screening-Services an, um die Sicherheit der Passwörter ihrer Kund:innen zu garantieren. Auch die deutsche SCHUFA[42] bietet ein entsprechendes kostenpflichtiges Service namens IdentSecure an.[43] Vermehrt wird Künstliche Intelligenz angewendet, um automatisiertes Betrugsmonitoring durchzuführen. KI-Systeme werden in vielen weiteren Bereichen wie der automatisierten Textverarbeitung (z. B. zur Analyse von Texten im Zusammenhang von Transaktionen), der Erkennung unerlaubter Zugriffe auf Systeme oder Schnittstellen (z. B. unter Nutzung falscher Identitäten) und zur Erkennung von Botnets verwendet.[44]

41 Fraunhofer-Institut für Arbeitswirtschaft und Organisation (IAO) (2021). KI zur Verhinderung von Identitätsbetrug. S. 15. http://publica.fraunhofer.de/dokumente/N-630686.html
42 SCHUFA steht für „Schutzgemeinschaft für allgemeine Kreditsicherung". Es handelt sich um eine deutsche Wirtschaftsauskunftei privatwirtschaftlichen Rechts.
43 SCHUFA IDentSecure, mySCHUFA (2022). https://www.meineschufa.de/de/identitaetsschutz
44 Fraunhofer-Institut für Arbeitswirtschaft und Organisation (IAO) (2021). KI zur Verhinderung von Identitätsbetrug. http://publica.fraunhofer.de/dokumente/N-630686.html

Leak Checker

Ebenfalls existieren eine Reihe an öffentlich zugänglichen Suchmaschinen wie ↗ https://haveibeenpwned.com/, die es Konsument:innen ermöglichen bekannte Data Leaks auf ihre Daten zu untersuchen. Konsument:in A kann mithilfe dieser Suchmaschinen nachsehen, ob ihre E-Mail-Adresse oder damit verbundene Passwörter in bekannten Leaks veröffentlicht wurden und diese Konten dann ggf. sichern. Problematisch ist hier jedoch, dass jede Person jede E-Mail-Adresse überprüfen kann – was datenschutzrechtliche Fragen aufwirft. Die Schattenseite dieser öffentlicher Leak-Checker ist also immer deren Missbrauch: Im Falle des „Ashley Madison"-Leaks, bei dem die Daten von tausenden Usern einer Seitensprungplattform veröffentlicht wurden, hatte dies massive Folgen für einige Betroffene. BBC berichtete 2015 von mit dem Leak zusammenhängenden Suiziden, da die persönlichen Daten von Personen, die auf der Plattform registriert waren, einsehbar und suchbar im Internet veröffentlicht wurden.[45]

Leak-Checker stellen aus Sicht des Datenschutzes ein Risiko dar, sofern jede Person jegliche E-Mail-Adressen, also auch jene anderer, frei eingegeben kann. Angesichts dieser Missbrauchsrisiken haben staatlich-geförderte Institutionen, die meist an Universitäten angebunden sind, ähnliche Leak-Checker entwickelt.[46] Diese senden das Ergebnis, ob ein Datensatz die eigene E-Mail-Adresse enthält, aber nur an die eingegebene Mail-Adresse selbst. Diese Leak Checker arbeiten meist nach ähnlichen Prinzipien: Sie suchen mithilfe von Crawlern kontinuierlich nach gestohlenen Passwort-Datensätzen im Internet und pflegen diese in die eigene Leak-Datenbank ein. Manche Anbieter von kostenpflichtigen Services wie beispielsweise Identeco folgen einem Privacy-by-Design Ansatz und ermöglichen einen DSGVO-konformen Datenabgleich, ohne selbst Kenntnis über die Identität der Betroffenen zu haben.[47]

Auch Konsument:innen können datenschutzkonform nachprüfen, ob eine ihrer E-Mail-Adressen in einem Leak aufgetaucht, oder ihr Passwort möglicherweise veröffentlicht wurde. Dazu gibt es beispielsweise die Website des Hasso Plattner Instituts: ↗ https://sec.hpi.de/ilc/ oder auch den Leak-Checker der Universität Bonn, in Kooperation mit Identeco: ↗ https://leakchecker.uni-bonn.de/.

5.2.2 Die Meldung von Identitätsdiebstahl bei Wirtschaftsauskunfteien

Wirtschaftsauskunfteien betreiben die Sammlung, Auswertung und Mitteilung von wirtschaftsrelevanten Daten über Unternehmen und Privatpersonen. Das betrifft meist Informationen über so genannte allgemeine Verhältnisse, welche die Seriosität und Zahlungsfähigkeit von Konsument:innen oder Unternehmen beschreiben. Empfänger:innen solcher Daten sind Geschäftspartner, die an diesen Informationen ein berechtigtes Interesse vorweisen können.[48] Insofern arbeiten in Österreich Wirtschaftsauskunfteien wie SCHUFA oder CRIF mit Händlern zusammen.

Derzeit können sich Betroffene von Identitätsmissbrauch initiativ bei Wirtschaftsauskunfteien melden. Damit leisten sie laut den Wirtschaftsauskunfteien einen Beitrag zur Sicherstellung, dass ihre missbräuchlich durch Dritte verwendeten Daten keine negativen Auswirkungen auf ihre Bonität nach sich ziehen. Sie können Auskunft über ihren Bonitätsscore verlangen. Es liegen keine Informationen dazu vor, in welchem Ausmaß dieses Angebot bereits in Anspruch genommen wird bzw. ob es als solches in der Praxis ein geeignetes, funktionierendes Instrument zur Schadenbegrenzung für Konsument:innen darstellt.

Die Wirtschaftsauskunftei SCHUFA etwa bietet mit dem SCHUFA-FraudPreCheck auch eine prädiktive Lösung für E-Commerce an.[49] Hierbei werden die Abhängigkeiten zwischen Transaktionen ausgewertet und es kann in Echtzeit entscheiden werden, ob

45 BBC. (2015) Ashley Madison: ‚Suicides' over website hack. https://www.bbc.com/news/technology-34044506
46 Hasso Plattner Institut. https://sec.hpi.de/ilc/search?lang=de
47 Identeco (2021). www.identeco.de
48 Virtuelles Datenschutzbüro, Wirtschaftsauskunfteien. (2022). https://www.datenschutz.de/wirtschaftsauskunfteien/
49 Fraunhofer IAO (2021).

eine Transaktion auffällig ist. Auch für Finanzdienstleister gibt es ein Service, den SCHUFA-FraudPool, über den sich Dienstleister gegenseitig von Betrug in Kenntnis setzen können. Die genannten Lösungen sind jedoch Services für Händler:innen. Für von Identitätsmissbrauch betroffene Konsument:innen bietet die SCHUFA mit meineSCHUFAplus ein kostenpflichtiges Paket zum Identitätsschutz an.[50]

Wirtschaftsauskunfteien haben eine zentrale Rolle, wenn es um die Schadensbegrenzung geht. Durch erweiterte Kooperationen im Bereich Datenaustausch mit Betreibern von Onlineshops könnte Betrug früher erkannt und möglicherweise verhindert werden. Maßnahmen, die auf engere Kooperation mit wirtschaftlichen Drittpartnern wie z. B. Wirtschaftsauskunfteien setzen, bedingen allerdings entsprechender Risikoabwägungen bezüglich des Missbrauchspotenzials von Black Lists und der Absicherung von möglichen Fehlerkorrektionen.

In diesem Zusammenhang ist zu betonen, dass Akteure der Privatwirtschaft ihr berechtigtes Interesse daran haben sich auf diese Weise zu schützen – für Konsument:innen vorteilhafter ist jedenfalls aber ein Ansprechpartner zur Vertretung der eigenen Interessen. Es erscheint insofern wichtig, dass der Austausch zwischen Wirtschaftsauskunfteien und dem Konsumentenschutz sowie anderen relevanten Stakeholdern forciert wird.

5.2.3 Die Beratung und Unterstützung von Betroffenen

Die Konsequenzen von Identitätsdiebstahl sind sehr unterschiedlich und für die Betroffenen teilweise erst graduell zu bemerken. Konsument:innen realisieren zunächst einzelne Probleme: die Forderung eines Inkasso-Büros, die Sperre ihres E-Mail-Accounts, unerklärte Abbuchungen auf ihrer Kreditkarte.

Für viele dieser Probleme von Konsument:innen gibt es bereits Anlaufstellen, an die sich Betroffene wenden. Hier zu nennen wären auch die Frauenberatungsstellen im Rahmen von Identitätsmissbrauch im Kontext eines Gewaltverhältnisses. In manchen Fällen, wie der Kompromittierung von Online-Accounts sind Plattformen die ersten Ansprechpartner.

Es bleibt jedoch meist nicht bei einem Problem, sondern es folgen weitere missbräuchliche Verwendungen der gestohlenen Identität. Hinzu kommt auch, dass es sich häufig um grenzüberschreitende Probleme handelt, bzw. in Extremfällen um Verbrechen mit schwerwiegenden Folgen und schwierigen Lösungswegen. In all diesen Fällen liegt die Last auf den Konsument:innen: Sie berichten von Problemen, die sich über Jahre hinweg nicht lösen lassen. Betroffene werden von Stelle zu Stelle geschickt, weil sich keiner verantwortlich fühlt. Dazu kommen Schwierigkeiten bei der Meldung von solchen Straftaten – die Erstattung einer Anzeige via der Meldestelle against Cybercrime (C4) ist derzeit beispielsweise noch nicht möglich. Erschwerend kommt hinzu, wenn Betroffene die Last der Beweiserbringung tragen müssen. Schließlich schaffen sie nur durch äußersten finanziellen, zeitlichen und psychischen Aufwand, der Spirale an Konsequenzen zu entkommen.

Betroffene von Identitätsdiebstahl nicht allein zu lassen, wäre wichtig. Der Blick nach Australien zeigt, wie die Unterstützung von Konsument:innen in der Hinsicht angeleitet und niederschwelliger werden kann. Auf der Website der australischen Regierung werden die Konsument:innen durch eine Schritt-für-Schritt Anleitung geführt.[51]

Die größten Unterschiede zur derzeitigen Situation in Österreich sind:

- (1) Sie können die Anzeige auch online erstatten und
- (2) mit der IDCARE steht ihnen eine Servicestelle zum Thema unterstützend zur Seite.[52]

Diese Form der niederschwelligen Unterstützung wäre auch in Österreich denkbar und könnte im

50 SCHUFA (2022). https://www.schufa.de/themenportal/20-01-datenklau-identitaetsmissbrauch-man-davor-schuetzen/
51 https://www.oaic.gov.au/privacy/data-breaches/identity-fraud
52 https://www.idcare.org/individuals

Rahmen eines von der öffentlichen Hand gesteuerten Dialogs zwischen den zentralen Akteuren stattfinden, die bereits jetzt teilweise mit Identitätsmissbrauch zu tun haben. Die verstärkte Kooperation zwischen Hilfsstellen für Betroffene, Ombudsstellen und Konsumentenschutzorganisationen würde einen Mehrwert für Konsument:innen bieten.

Überlegt werden könnte die Einrichtung von einer Melde- und Beratungskompetenzstelle zu Identitätsdiebstahl, welche die erste Anlaufstelle für Betroffene wäre und zwischen Plattformen, Strafverfolgungsbehörden, Wirtschaftsauskunfteien, Inkassobüros und Betroffenen vermitteln könnte. Eventuell könnte in Extremfällen den Betroffenen auch die Last von hohen Anwaltskosten und Beratungshonoraren abgenommen werden. Zu bedenken ist, dass es sich dabei um eine anspruchsvolle Beratungstätigkeit aus technischer, rechtlicher und psychologischer Sicht handelt.

In dem Zusammenhang diskutiert werden sollte auch, ob das Erstatten von Anzeige in diesen Fällen erleichtert werden kann. Derzeit ist es in Österreich noch nicht möglich diese digital, beispielsweise via der Meldestelle against Cybercrime zu stellen. Gleichzeitig ist das Thema Identitätsdiebstahl kompliziert und fordert von Beamten auf Polizeidienststellen viel ab, wenn es darum geht die Betroffenen umfassend zu beraten. Die digitale Abwicklung sowie die Einrichtung einer zentralen Kompetenzstelle könnte hierbei Abhilfe leisten.

6. Ausblick

Wohin kann ich mich wenden, wenn ich Opfer von Identitätsmissbrauch bin? Auf diese einfache Frage gibt es derzeit keine klare Antwort, obgleich die Konsequenzen für Betroffene einschneidend sein können. Grund dafür ist die breite Streuung der Folgen und die entsprechend vielen Akteure als mögliche Ansprechpersonen zur Minimierung des Schadens: z. B. bestimmte Plattformen, Beratungsstellen zu Gewalt, die Polizei, Banken, Wirtschaftsauskunfteien, etc.

Derzeit obliegt es dem Opfer sich im Falle des Falles auf die Suche nach der geeigneten Ansprechperson zu machen, um den Schaden zu minimieren. In extremen Fällen heißt dies für Konsument:innen eine jahrelange massive finanzielle und psychische Belastung. Angesichts dessen erscheint die Schaffung einer zentralen Anlaufstelle für Konsument:innen als eine sinnvolle Maßnahme. Dies bedarf jedoch weiterer Überlegungen.

Dem vorangestellt werden muss der Dialog zwischen den zentralen Akteuren zum einen zur Abschätzung des Ausmaßes und zum anderen der Eruierung von effektiven Wegen der engeren Zusammenarbeit in Fällen von Identitätsmissbrauch. Was können Social Media-Plattformen unternehmen, um z. B. aus dem eigenen Konto ausgesperrte Betroffene von Identitätsdiebstahl zu unterstützen? Wie können Wirtschaftsauskunfteien im Sinne der Konsument:innen bei Problemen durch Bestellbetrug handeln? Wie können Betroffene es verhindern immer wieder von Strafbehörden als Folge eines Identitätsmissbrauchs kontaktiert zu werden? An einen Tisch gebracht müssen u. a. Vertreter:innen aus Konsumentenschutz, Wirtschaftauskunfteien, Inkasso-Büros, Banken, aus dem E-Commerce und von relevanten Plattformen.

Naheliegend ist bei Identitätsmissbrauch aufgrund der zentralen Bedeutung von Daten in diesen Fällen an technische Lösungen zu denken. Die Einführung von Sicherheitsmaßnahmen wie Identitätsfeststellungen sind jedoch immer in Abwägung der Interessen von Verbraucher:innen an Anonymität und an Schutz zu sehen. Sie sollten nicht in einer überschießenden Kontrolle von Verbraucher:innen münden.

Eine Dunkelfeldstudie zum Ausmaß von Identitätsdiebstahl in Österreich wäre dafür vonnöten. Wie hoch ist der bezifferte Schaden durch den Missbrauch an Daten für Bestellbetrug? In welchen Bereichen kommt es gehäuft zu Identitätsmissbrauch und wo braucht es Regulierung? Anders gefragt: Wann ist eine zweifelsfreie Identitätsklärung aus Sicht von Verbraucher:innen notwendig? Maßnahmen gegen Identitätsmissbrauch müssen grundrechtssensibel gestaltet werden. Nur so wird eine zielsichere und effektive Ergreifung von Maßnahmen sichergestellt, die mehr Sicherheit für Konsument:innen vor Identitätsdiebstahl – unter Berücksichtigung ihrer Interessen an Privatsphäre und Identität, bietet.

Im Rahmen dieser Studie erscheint es deshalb zentral, dass Akteure und Anlaufstellen, die bereits heute teilweise mit Opfern von Identitätsdiebstahl zu tun haben, in ihrem Bemühen koordiniert vorgehen und daran gearbeitet wird, eine niederschwellige Form der Unterstützung für Betroffene anzubieten. Angelehnt an z. B. das australische Modell wäre anzudenken, dass eine Melde- und Beratungskompetenzstelle von der öffentlichen Hand initiiert wird. Für Betroffene wäre eine proaktive Bearbeitung des sich ausweitenden Problems Identitätsdiebstahl von großer Bedeutung.

7. Wie kann ich mich gegen Identitätsmissbrauch schützen?

Vorsicht bei E-Mails von unbekannten Absender:innen!
Klicken Sie nicht auf unbekannte Links, öffnen oder installieren Sie keine unbekannten Dateien oder Programme. Vorsicht geboten ist auch bei unbekannten SMS oder anderen Nachrichten.

Software-Updates nicht vergessen!
Achten Sie auf regelmäßige Software-Updates und halten Sie Ihren Anti-Viren-Schutz auf dem aktuellen Stand.

Benutzen Sie starke Passwörter!
Besonders sicher sind Sie mit einem Passwortmanager.

Vorsicht beim Teilen von persönlichen Infos!
Seien Sie sparsam mit dem Veröffentlichen und Mitteilen von persönlichen Informationen. Nutzen Sie die Privatsphäre-Einstellungen und bedenken Sie, wer wieviel über Ihr Privatleben erfährt.

Lassen Sie sich von Logos und Design nicht täuschen!
Verlassen Sie sich nicht auf bekannte Logos und das Design von E-Mails oder Websites. Überprüfen Sie stets, ob Sie sich auf der echten Website befinden, bevor Sie Zugangsdaten eingeben.

Achtung beim Verwenden von öffentlichen Computern!
Loggen Sie sich nicht von öffentlichen Computern in wichtige Onlinekonten ein. Speichern Sie Ihre Passwörter nicht im Internet-Browser, diese könnten sonst von Kriminellen ausgelesen werden.

Löschen Sie alte Konten!
Löschen Sie Konten, die Sie nicht mehr verwenden. Das minimiert die Chance, dass Ihre Daten im Falle eines Leaks veröffentlicht werden.

Werden Sie proaktiv!
Suchen Sie nach Ihrem Namen im Internet, überprüfen Sie regelmäßig Ihre Kontoauszüge und Kreditkartenabrechnungen und nutzen Sie einen Leak-Checker!

8. Ich bin betroffen, was ist zu tun?

Tipps für die häufigsten Fälle von Identitätsmissbrauch sind hier aufgeführt.[53]

Es besteht das Risiko, dass jemand unrechtmäßig Zugriff zu Ihrem Onlinekonto hat

Wenn eines oder mehrere Ihrer Onlinekonten kompromittiert sind, sollten Sie folgende Schritte rasch durchführen:

- **Stellen Sie rasch sicher, welche Konten betroffen sind:** Wo verwenden Sie dieselbe E-Mail-Adresse oder dasselbe Passwort? All diese Konten könnten betroffen sein.
- **Ändern Sie die Passwörter in der richtigen Reihenfolge:** Sichern Sie zuerst das Passwort für das Konto, das Sie zur Wiederherstellung von anderen verwenden (meist der E-Mail-Account). Ändern Sie erst danach andere Passwörter. Facebook- oder Google-Accounts werden häufig auch für die Nutzung anderer Onlinedienste verwendet. Ändern Sie jedenfalls auch die Passwörter dieser Accounts, um mögliche Risiken zu minimieren.
- **Verwenden Sie für jeden Account ein eigenes, starkes Passwort:** Stellen Sie sicher, dass Sie nicht dasselbe Passwort für viele Konten verwenden. Abhilfe schafft hier ein Passwortmanager, den Sie auf allen Ihren Geräten installieren können. Zudem ist es ratsam die Zwei-Faktor-Authentifizierung für wichtige Konten wie E-Mail zu verwenden.
- **Kontrollieren Sie Ihre Konto-Einstellungen:** Versichern Sie sich, dass die Einstellungen Ihrer Onlinekonten nicht verändert worden sind, achten Sie auch auf Weiterleitungen an fremde Accounts oder möglicherweise von Dritten erstellte Rückfalloptionen. Korrigieren Sie diese Einstellungen gegebenenfalls.

Es werden Bestellungen in Ihrem Namen durchgeführt oder Ihr Ausweis wird für strafrechtliche Aktivitäten verwendet

Wurde Ihr Ausweis gestohlen und kommt es zu strafrechtlichen Problemen, kann es notwendig werden sich gegebenenfalls auch anwaltliche Unterstützung zu suchen. In den meisten Fällen kann allerdings über eine Anzeige bei der Polizei und der Kommunikation des Falles mit involvierten Online-Shops, Inkasso-Büros, Social Media-Plattformen die Situation geklärt werden.

- **Erstatten Sie eine Anzeige der Polizei:** Aus der Praxis wissen wir, das ist nicht immer einfach, aber bestehen Sie jedenfalls auf eine Aufnahme Ihres Falles. Mit dieser Anzeige können Sie gegenüber anderen glaubhaft machen, Opfer von Identitätsmissbrauch zu sein.
- **Reagieren Sie umgehend auf unbegründete Forderungen:** Informieren Sie sich, ob es sich um eine die Forderung eines legitimen Online-Shops bzw. Inkasso-Büros handelt. Wenden Sie sich mit einer Klarstellung an den Online-Shop oder das Inkasso-Büro.
- **Eruieren Sie, auf welcher Basis in Ihrem Namen gehandelt wird:** Ändern Sie umgehend Ihre Passwörter und beantragen Sie ggf. eine neue Kreditkarte. In extremen Fällen kann es hilfreich sein, sich bei Wirtschaftsauskunfteien zu melden, um negative Auswirkungen auf die Bonitätseinschätzung zu verhindern.

53 BSI (2022). Identitätsdiebstahl – Hilfe f. Betroffene. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Infizierte-Systeme-bereinigen/Infektionsbeseitigung-bei-Smartphones-und-Tablets/infektionsbeseitigung-bei-smartphones-und-tablets_node.html , https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Identitaets-diebstahl/Hilfe-fuer-Betroffene/hilfe-fuer-betroffene.html

Der direkte Weg zu unseren Publikationen:
E-Mail: konsumentenpolitik@akwien.at

Bei Verwendung von Textteilen wird um Quellenangabe und Zusendung
eines Belegexemplares an die AK Wien, Abteilung Konsumentenpolitik, ersucht.

Impressum

Medieninhaber: Kammer für Arbeiter und Angestellte für Wien,
Prinz-Eugen-Straße 20–22, 1040 Wien, Telefon: (01) 501 65
Offenlegung gem. § 25 MedienG: siehe wien.arbeiterkammer.at/impressum
Zulassungsnummer: AK Wien 02Z34648 M
AuftraggeberInnen: AK Wien, Konsumentenpolitik
Durchführung im Auftrag der AK Wien: ÖIAT (Österreichisches Institut für
angewandte Telekommunikation)
Grafik Umschlag und Druck: AK Wien
Verlags- und Herstellungsort: Wien
© 2022: AK Wien

Stand April 2022
Im Auftrag der Kammer für Arbeiter und Angestellte für Wien

GERECHTIGKEIT #FÜRDICH

Gesellschaftskritische Wissenschaft: die Studien der AK Wien

Alle Studien zum Download:
wien.arbeiterkammer.at/service/studien