Leitblatt

Identitätsmissbrauch

Bundesverband

Charakteristika von Identitätsmissbrauch

- Beim Identitätsdiebstahl werden personenbezogene Daten wie das Geburtsdatum, die Adresse, Bankkonten, Kreditkartennummern, Führerschein- oder Sozialversicherungsnummern entwendet.
- Solch einem Diebstahl folgt meist ein Identitätsmissbrauch, indem eine unbefugte Person mit diesen personenbezogenen Daten die Identität einer anderen Person annimmt.
- Im digitalen Raum kann dies geschehen durch das illegale Eindringen in
  - Profile auf sozialen Webseiten (oder sogar Erstellung eines Duplikates),
  - E-Mail-Accounts (z.B. zur Versendung von Nachrichten an das Adressbuch mit Hilferuf und der Bitte um Geldsendung oder Anforderung neuer Passwörter),
  - Versandhandel-Konten zum Kauf von Waren.
- Das Ziel können Rufschädigung, Betrug oder andere illegale Aktivitäten sein, verbunden mit hohen Schulden und Strafen für das Opfer.

Dem Diebstahl und Betrug vorbeugen

- Vernichten Sie Dokumente oder Ihre Post gründlich und schmeißen Sie diese nicht einfach in den Müll.
- Seien Sie nicht zu offenherzig mit der Weitergabe von Fotos, Geburtsdatum aber auch anderen privaten Daten, v.a. auch auf Ihren Netzwerkprofilen.
- Seien Sie vorsichtig und restriktiv bei der Herausgabe Ihrer Ausweisdokumente und hinterfragen Sie rechtliche Notwendigkeiten, wenn Kopien von Ihrem Ausweisdokument angefertigt werden (Geldwäschegesetz, Anti-Terror-Gesetz).
- Achten Sie nach Veranstaltungen darauf, das Namenschild abzunehmen.
- Tragen Sie Ihre Firmen-ID-Karten außerhalb des Firmengeländes (z.B. auf dem Weg ins nächste Restaurant) nicht offen sichtbar.

Digital

- Loggen Sie sich nie über ungesicherten WLAN-Netze mit Ihrem Benutzernamen oder Passwort ein! – Dies kann leicht ausgelesen werden. Vergessen Sie nicht das Deaktivieren des automatischen Logins.

- Installieren Sie Virenschutzprogramme auf Laptop, Smartphone und Tablet usw. und aktualisieren Sie diese regelmäßig.
- Verwenden Sie sichere Kennwörter [1] und speichern Sie diese nicht im Browser.
- Achten Sie auf sichere und seriöse Internetseiten (Beginn mit https, Schlüsselsymbol) und auf deren Datenschutzrichtlinien.
- Suchen Sie Ihren Namen ab und zu über Suchmaschinen im Web und überprüfen Sie regelmäßig Ihre sozialen und beruflichen Netzwerkprofile.
- Viele Apps für Smartphones greifen auf Ihre privaten Daten zu. Kontrollieren Sie vor Installation einer App, welche Zugriffsrechte die App auf welche Ihrer Daten einfordert.

Was tun, wenn es geschehen ist?

- Erstatten Sie auf jeden Fall Anzeige bei der Polizei!
- Ändern Sie **alle** Ihre Zugangsdaten.
- Benachrichtigen Sie den Anbieter (Onlineshop usw.) und Ihr Bank- und Kreditinstitut.
- Legen Sie Widerspruch gegen Inkassobescheide ein. Lassen Sie sich bei der Schufa oder anderen Auskunfteien als Opfer von Identitätsdiebstahl registrieren (z.B. www.schufa.de/identitaetsschutz).

[1] Je mehr Zeichen und Variation in Klein- und Großbuchstaben sowie Sonderzeichen und Ziffern desto besser. Um sich dies besser zu merken, bauen Sie sich Eselsbrücken, z.B. indem Sie einen Satz zur Hilfe nehmen: „Ich bin jeden Morgen um 8 Uhr im Büro!“ ergibt das Passwort „IbjMu8UiB!“.

ASW Bundesverband

Herausgeber: ASW Bundesverband – Allianz für Sicherheit in der Wirtschaft e. V.
Stand: Februar 2017 | **Kontakt:** info@asw-bundesverband.de