Hessischer Beauftragter für Datenschutz und Informationsfreiheit

Umgang mit Identitätsdiebstahl – Erkennen, Reagieren, Vorbeugen

Durch die fortschreitende Digitalisierung und die Nutzung unterschiedlicher Internetdienste wie beispielsweise privater oder kommerzieller Webseiten, Internetforen oder sozialer Netzwerke geben Nutzerinnen und Nutzer an vielen Stellen im Internet private Daten zu ihrer Person preis. Erhalten Unbefugte Einsicht in diese personenbezogenen Daten, beispielweise nach einem erfolgreichen Angriff auf einen Internetdienst, so können sie die erbeuteten Daten für etwaige kriminelle Handlungen nutzen. Je nach Art der Daten können Täter zum Beispiel auf Kosten der Betroffenen Verträge abschließen oder Einkäufe tätigen, Angehörige der Betroffenen schädigen („Enkeltrick") oder die Daten zur Bloßstellung oder Erpressung der Betroffenen nutzen.

Identitätsdiebstahl erkennen

Da der Missbrauch personenbezogener Daten auf viele Arten möglich ist, sind die Folgen für die Betroffenen selten direkt erkennbar. Mögliche Indizien für einen Identitätsmissbrauch sind etwa:

- Sie erhalten Zahlungsaufforderungen für Bestellungen, die sie nicht getätigt haben.
- Das Einloggen bei einem Internetdienst, dem E-Mail-Anbieter oder bei einem sozialen Netzwerk ist trotz vermeintlich korrektem Passwort nicht möglich.
- In ihrem Namen werden Beiträge im Internet veröffentlicht, E-Mails versendet oder Profile in sozialen Netzwerken erstellt.
- Sie erhalten von ihrem Dienstleister eine Benachrichtigung, dass ein neues Gerät für den Dienst registriert wurde oder sie den Dienst von einem ungewöhnlichen Ort genutzt haben, ohne dass dies tatsächlich der Fall ist.

Zu beachten ist, dass nicht jede verdächtige Aufforderung, wie beispielsweise eine Rechnung, eine Mahnung oder ein Aufruf zum Passwortwechsel auf einen Identitätsdiebstahl zurückzuführen ist. Kriminelle können solche Aufforderungen im Rahmen von Spam- oder Phishing-Angriffen verwenden, um sich als vertrauenswürdiger Kommunikationspartner auszugeben und die Betroffenen zur Ausführung einer schädlichen Aktion, wie etwa der Installation einer Schadsoftware oder Preisgabe von Zugangsdaten, zu bewegen. Die Glaubwürdigkeit einer Aufforderung sollte daher stets sorgfältig geprüft werden, insbesondere wenn diese Aufforderung per E-Mail eingegangen ist.

Eine Möglichkeit zur Prüfung, ob eigene personenbezogene Daten aus Internetdiensten Dritten zugänglich wurden, etwa im Rahmen eines Cyberangriffs, bieten Dienste wie der Identity Leak Checker des Hasso-Plattner-Instituts. Dieser Dienst *https://www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/StraftatenImInternet/Identitaetsdiebstahl/identitaetsdiebstahl_node.html* prüft auf Basis einer angegebenen E-Mail-Adresse, ob diese mit personenbezogenen Daten, die im Rahmen eines bekanntgewordenen Angriffs von Kriminellen erbeutet wurden, im Zusammenhang steht. Ein positives Ergebnis zeigt, von welchem Dienst die personenbezogenen Daten stammen, es bedeutet jedoch nicht zwingend, dass ein Identitätsmissbrauch bereits stattgefunden haben muss.

Zu beachten ist, dass der Identity Leak Checker nur E-Mail-Adressen kennt, die in Zusammenhang mit bekanntgewordenen Angriffen oder anderen Datenveröffentlichungen stehen. Personenbezogene Daten können eventuell auch im Rahmen eines unbekannten Angriffes entwendet worden sein. Ein „negatives" Ergebnis des Checks liefert demnach keine absolute Sicherheit, dass es zu keinem Identitätsdiebstahl gekommen ist. Bei einem „positiven" Ergebnis ist in jedem Fall Handlungsbedarf gegeben – siehe dazu im Folgenden mehr.

Auf Identitätsdiebstahl reagieren

Stellen Betroffene fest, dass ihre personenbezogenen Daten gestohlen wurden oder bereits missbraucht werden, sollten sie unverzüglich handeln. Um Betroffenen mögliche Gegenmaßnahmen im Falle eines Identitätsdiebstahls aufzuzeigen, hat das Bundesamt für Sicherheit in der Informationstechnik eine Hilfestellung für Betroffene veröffentlicht.

Prävention von Identitätsdiebstahl

Nutzerinnen und Nutzer sollten darauf achten, dass sie seriöse Anbieter nutzen, kritisch prüfen, welche personenbezogenen Daten sie von sich preisgeben, und kontrollieren, ob die Sicherheitsvorkehrungen zum Schutz ihrer Daten ausreichend sind. So sollten zum Beispiel Zugangsdaten wie etwa Passwörter zu jedem genutzten Dienst einzigartig sein. Wo möglich sollte mit einer Zwei-Faktor-Authentisierung gearbeitet und Dienste, die keine geschützte Verbindungen über HTTPS bzw. Transport Layer Security (TLS) anbieten, gemieden werden.

Ein sparsamer und bedachter Umgang mit den eigenen Daten im Internet ist die beste Vorbeugung gegen Identitätsdiebstahl und Identitätsmissbrauch. Generell gilt: Daten, die Nutzerinnen und Nutzer von sich nicht preisgeben, können auch nicht missbraucht werden.

Weitere Maßnahmen zur Prävention von Identitätsdiebstahl sind auf den Seiten des Bundeskriminalamtes und des Bundesamtes für Sicherheit in der Informationstechnik aufgelistet.

https://www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/StraftatenImInternet/Identitaetsdiebstahl/identitaetsdiebstahl_node.html

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Identitaetsdiebstahl/Schutzmassnahmen/schutzmassnahmen_node.html