14796/J XXVII. GP

Eingelangt am 30.03.2023

Anfrage

der Abgeordneten Mag. Christian Drobits und Genoss:innen

an die Bundesministerin für Justiz

betreffend Identitätsdiebstahl

Identitätsdiebstahl im Internet ist aufgrund immer wieder erfolgender groß angelegter „Hackerangriffe“ bzw. „Datenschutzpannen“ ein zunehmendes Problem. „Diebstahl, Handel und Missbrauch mit gestohlenen Daten haben sich zu einem lukrativen Geschäft für Cyberkriminelle entwickelt. Der Identitätsdiebstahl erfolgt mittlerweile überwiegend über Schadsoftware-Infektionen und weitgehend unbemerkt für die betroffenen Anwenderinnen und Anwender. Aber auch Phishing-E-Mails und Phishing-Webseiten tragen ihren Teil dazu bei, dass persönliche Daten immer häufiger in die Hände Unbefugter gelangen.“ (Onlinesicherheit - Identitätsdiebstahl)

Neben Datendiebstählen im großen Stil (Dataleaks oder Databreaches auf sozialen Plattformen, bei E-Mail-Anbietern, etc) können auch Phishing über gefälschte E-Mails, gefälschte Websites, E-Mails bzw. Messenger-Nachrichten, SMS oder Anrufen bzw. betrügerische Online-Shops Ursachen für Identitätsdiebstahl sein. Die so gestohlenen Daten finden bei unterschiedlichen kriminellen Aktivitäten Anwendung – vom Betrug bis hin zur Geldwäsche oder zur Unterstützung terroristischer Netzwerke. Oft genügen schon der Name, das Geburtsdatum und die Adresse einer Person, um in fremdem Namen Bestellungen aufzugeben, die Produkte abzufangen oder an abweichende Lieferadressen schicken zu lassen. Die vom Identitätsdiebstahl Betroffenen erhalten falls überhaupt nur die Rechnung oder sogar Forderungen eines Inkassobüros, aber keine Leistung. Eine weitere Form des

Identitätsdiebstahls ist in sozialen Netzwerken mit dem Missbrauch von Onlinekonten und der Erstellung von Fake-Profilen zu beobachten.

Im Jahr 2019 gaben bereits rund elf Prozent der Österreicher:innen an, dass sie schon einmal von Identitätsdiebstahl betroffen waren. Die Konsequenzen für Einzelne können massiv sein, denn die gestohlenen Daten werden ua. auch für kriminelle Aktivitäten genutzt. Die Daten werden z. B. missbraucht, um Bestellungen zu tätigen und teilweise auch 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. (Identitaetsdiebstahl.pdf (arbeiterkammer.at)

Die unterzeichneten Abgeordneten stellen daher nachstehende

Anfrage:

1. Wie hoch war die Anzahl an Identitätsdiebstählen in Österreich in den letzten 5 Jahren? Wie viele Anzeigen wegen Identitätsdiebstahl liegen bei den Landeskriminalämtern in den Bundesländern auf? Wie viele davon wurden verfolgt (bitte nach Jahren und Bundesländern gegliedert anführen)

2. Die gemeldeten/angezeigten Identitätsdiebstähle zeigen nur einen Teil der Fälle auf; mit welcher Dunkelziffer ist bei Identitätsdiebstählen in Österreich zu rechnen?

3. Liegen Ihrem Ressort Daten dazu vor, in welchen Bereichen es gehäuft zu Identitätsmissbrauch kommt? In welchen Bereichen besteht aus Sicht Ihres Ressorts im Konnex mit Identitätsmissbrauch Bedarf nach stärkeren Regulierungen?

4. Aktuell gibt es in Österreich keinen eigenen Straftatbestand für Identitätsdiebstahl; allerdings begehen Betrüger im Netz dabei andere Vergehen, die laut Strafgesetzbuch (StGB) verfolgt werden können. Nach welchen gesetzlichen Regelungen/Tatbeständen

wird Identitätsdiebstahl in Österreich geahndet?

5. Besteht aus Sicht Ihres Ressorts Bedarf nach Präzisierung des gesetzlichen Rahmens zum Identitätsdiebstahl und wenn ja, welcher?

6. Wie viele Verfahren im Zusammenhang mit Identitätsdiebstahl waren in den letzten 5 Jahren zu verzeichnen? Zu wie vielen Verurteilungen/Strafen kam es dabei? (bitte nach Jahren und Bundesländern aufgliedern)

7. Wie hoch kann der jährliche Schaden durch Identitätsdiebstahl in Österreich beziffert werden?

8. Welche Maßnahmen werden seitens ihres Ressorts neben der geplanten Verschärfung der Strafen für Cybercrime-Delikte zur verstärkten Bekämpfung des Identitätsdiebstahls verfolgt bzw. gesetzt?

9. Artikel 33 DSGVO sieht bei Verletzung des Schutzes personenbezogener Daten eine Meldepflicht für den Verantwortlichen binnen 72 Stunden nach Bekanntwerden bei der Aufsichtsbehörde vor. Bedeutet die Datenpanne „voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten“ des Betroffenen, so ist der Betroffene unverzüglich gem. Art. 34 DSGVO von der Datenschutzverletzung „in klarer und einfacher Sprache“ zu unterrichten. In der Praxis erreichen die Benachrichtigungen die betroffenen Konsument:innen oft erst einige Monate oder sogar Jahre nach dem eigentlichen Data Leak. Welche Maßnahmen wären aus Sicht Ihres Ressorts möglich und zu setzen, um die Information der betroffenen Konsument:innen zu verbessern?

10. Von Identitätsdiebstahl Betroffene haben mit einer Vielzahl unterschiedlicher Probleme zu kämpfen, deren Behebung überaus zeit- und kostenintensiv sein kann. Ist aus Ihrer Sicht die Einrichtung niederschwelliger Unterstützungsangebote für Betroffene von Identitätsdiebstahl zu forcieren, wie zB. die Einrichtung einer Melde- und Beratungskompetenzstelle zu Identitätsdiebstahl, welche als erste Anlaufstelle für Betroffene fungiert und die zwischen Plattformen, Strafverfolgungsbehörden,

Wirtschaftsauskunfteien, Inkassobüros und Betroffenen vermitteln könnte?

11. Von Identitätsmissbrauch/-diebstahl Betroffene können sich aktuell initiativ an Wirtschaftsauskunfteien wenden und Auskunft über ihren Bonitätsscore verlangen, damit ihre missbräuchlich durch Dritte verwendeten Daten keine negativen Auswirkungen auf ihre eigene Bonität nach sich ziehen. Liegen Ihrem Ressort Daten vor, in welchem Ausmaß dieses Angebot in Anspruch genommen wird?