RheinlandPfalz
LANDESKRIMINALAMT

Handlungsempfehlung zum „Identitätsdiebstahl“

Mainz, 05.01.2019

Mit den nachfolgenden Ausführungen möchte das Landeskriminalamt Rheinland-Pfalz Ihnen Informationen im Zusammenhang mit dem Phänomen „Identitätsdiebstahl“ zur Verfügung stellen.
Die Handlungsempfehlung dient einer Verbesserung der Handlungssicherheit ohne dabei bindenden Charakter zu entfalten.
Unter digitaler Identität werden personenbezogene Daten des einzelnen Nutzers sowie dessen Aktivitäten im Internet umfasst. Hierzu zählen alle Arten von Nutzerdaten und zahlungsrelevante Informationen in den Bereichen

- Kommunikation (z.B. E-Mail-Verkehr / Soziale Netzwerke)
- E-Commerce (z.B. Onlinebanking / Onlinebrokerage / Onlineportale)
- E-Government
- Berufsspezifische Informationen
- Cloud-Computing
- Zahlungsverkehr (z.B. Kreditkartendaten / Zahlungsdaten).

Die Bandbreite des Missbrauchs kann hierbei von der Bestellung von Waren in Online-Shops, der fälschlichen Nutzung des Namens in Blogs und Foren, der Erstellung falscher Profile in sozialen Netzwerken bis hin zur Begehung von Straftaten zum Nachteil Dritter reichen.
Häufig sammeln der oder die Täter zunächst die Daten und verwenden diese erst später für ihre eigenen illegalen Aktivitäten bzw. verkaufen die gestohlenen Daten im Darknet weiter. Der Identitätsdiebstahl und die in der Regel damit verbundene Infizierung des Rechners bleiben häufig unentdeckt.
Die Täter gelangen auf unterschiedlichste Weise an Ihre digitalen Daten, wie beispielsweise über

- Recherche in öffentlich zugänglichen Quellen (z.B. Google-Suche)

- Hacking Ihres persönlichen Profils oder des persönlichen Profils einer Ihnen bekannten Person, die zu Ihnen Kontakte hat
- Schadprogramme / Malware, die in vermeintlich nützlichen Programmen integriert sind, die Sie sich herunterladen
- Installation von Schadcode auf Ihrem Rechner nach Besuch einer kompromittierten Webseite (Drive-by-Exploits)
- Phishing-Mails, mit denen Sie aufgefordert werden, Ihre digitale Identitäten auf verlinkte und oftmals gefakte Webseiten einzugeben
- Spyware-Programme, welche im Hintergrund heimlich Informationen über Sie sammeln und weiterleiten
- Hacken von Servern, auf denen Ihre Nutzerinformationen gespeichert sind.

Handlungsempfehlungen zum Schutz Ihrer digitalen Identität

Neben einem restriktiven Umgang mit Ihren digitalen Daten im Internet und in Sozialen Netzwerken, der Nutzung vielschichtiger Verteidigungssysteme (bspw. bestehend aus Firewalls, Antispam-Software sowie Antivirenprogrammen, der regelmäßigen Durchführung von Software-Updates und Backups zur Datensicherung sollten Sie insbesondere nachfolgende Maßnahmen durchführen:

Account:

- Prüfen Sie, ob Ihre eigenen Accounts mithilfe von öffentlich zugänglichen Informationen (z.B. Beantwortung von Sicherheitsfragen[1] zum Zugriff oder dem Zurücksetzen des Passworts) angreifbar sind
- Prüfen Sie, ob eigene Accounts bereits in öffentlich gewordenen Leaks[2] enthalten sind
- Prüfen Sie die angegebene letzte Login-Zeit immer auf Plausibilität (z.B. fehlgeschlagene Logins, Logins über unbekannte Geräte, parallele Sitzungen)
- Prüfen Sie, ob Daten (z.B. für Backups / Fotoalben) automatisch zu Cloud-Diensten hochgeladen werden und deaktivieren Sie diese Funktion oder meiden Sie diese für Ihre sensiblen Daten.

[1] Z.B. Abfrage des Wohnortes
[2] Auswahl v. Leak-Datenbanken zur Recherche:
https://sec.hpi.de/ilc/ https://haveibeenpwned.com/ https://monitor.firefox.com/ https://breachalarm.com/

Passwörter:

- Verwenden Sie bei jedem Account ein anderes sicheres (starkes) Passwort und ändern Sie dieses in regelmäßigen Abständen. Eine höhere Sicherheit bieten bspw. die Zwei-Faktor-Authentifizierungen[3] sofern diese vom Anbieter bereitgestellt wird. Wechseln Sie ggf. zu einem Anbieter, der diese unterstützt.

Verschlüsselung:

- Verschlüsseln[4] Sie Ihre Daten und nutzen Sie, sofern möglich, verschlüsselte Übertragungswege

Apps:

- Laden Sie Programme und Apps nur aus Originalquellen bzw. legalen App-Stores herunter. (Vor der Installation sollte eine entsprechende Überprüfung der Programme mittels Antivirensoftware durchgeführt werden)
- Überprüfen Sie, ob Apps automatisiert Kontaktlisten zum Anbieter übermitteln. Meiden Sie diese bzw. nutzen Sie diese nicht für sensible Daten

WLAN:

- Nutzen Sie im öffentlichen WLAN verschlüsselte VPN-Tunnel, um ein Ausspähen von Informationen zu verhindern
- Führen Sie keine sensiblen Transaktionen über öffentliche Hotspots durch

Drahtlosverbindungen

- Deaktivieren Sie Drahtlosverbindungen und GPS bei Nicht-Nutzung.

E-Mails:

- Überprüfen Sie alle E-Mails auf die richtige Absenderadresse sowie die korrekte Schreibweise der E-Mail Domain

[3] BSI: Zwei-Faktor-Authentisierung bezeichnet die Kombination von zwei Authentisierungstechniken, wie Passwort plus Transaktionsnummern (Einmalpasswörter) oder plus Chipkarte.
https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Glossar/glossar_node.html

[4] BSI: Wie verschlüsselt kommunizieren?
www.bsi-fuer-buerger.de [...] Verschluesselung

- Seien Sie bei Eingang von E-Mails von unbekannten Absendern mit Anhängen oder Links besonders achtsam - es könnte sich um Schadcode handeln

Rechtlicher Hinweis

Der Identitätsdiebstahl an sich stellt keine eigene Straftat dar.
Es werden jedoch je nach Fallart Straftaten, wie beispielsweise das Abfangen von Daten, das Ausspähen von Daten, die Fälschung beweiserheblicher Daten und der Computerbetrug, erfüllt.
Wir raten Ihnen bei Vorliegen des Verdachts eines Identitätsdiebstahls umgehend zu reagieren und eine Anzeige bei Ihrer örtlich zuständigen Polizeidienststelle zu erstatten. Die für Ihren Wohnsitz in Rheinland-Pfalz zuständige Polizeidienststelle können Sie über die Suchmöglichkeit in unserer Dienststellendatenbank[5] erlangen. Durch die Eingabe Ihrer Suchbegriffe erhalten Sie Auskunft, welche Polizeidienststelle zuständig ist

Woran Sie bei der Anzeigenerstattung denken sollten:

- Machen Sie genaue Angaben zur Tat, Tatzeit, Feststellungszeit, zum Schaden, zum Speicherort der „gestohlenen“ Daten und zur Vorgehensweise der Täter / Tatverdächtigen (verwendete Methode zum Ausspähen Ihrer digitalen Daten)
- Machen Sie Angaben zu bereits eingeleiteten Maßnahmen
- Fertigen Sie Screenshorts von besuchten Internetseiten und notieren Sie sich die Adressen von gefälschten Webseiten (sofern vorhanden)
- Sichern Sie alle elektronisch vorliegenden Unterlagen auf CD und übergeben Sie diese an die Polizei
- Bei Verdacht auf Schadsoftware auf Ihrem System:
    - Stellen Sie ggf. vorliegende schriftliche Unterlagen in Papierform ebenfalls der Polizei zur Verfügung
    - Machen Sie Angaben zu Ihrem PC-Betriebssystem und der genutzten Antiviren-Software
    - Ggf. wird Ihr Rechner oder Smartphone zur Identifizierung der darauf befindlichen Schadsoftware benötigt.

[5] Link: https://www.polizei.rlp.de/de/dienststellensuche/

Beratungsangebot:

Sie können sich zusätzlich bei unseren polizeilichen Beratungsstellen[6] zu den unterschiedlichsten Fragen kompetent, neutral und kostenfrei beraten lassen. Hier stehen Fachkräfte zur Verfügung, die Auskünfte und Hilfe zu Themen der polizeilichen Prävention, der Verkehrsunfallprävention oder zum Thema Opferschutz geben. Vereinbaren Sie einen Termin unter der jeweiligen angegebenen Rufnummer oder nutzen Sie die entsprechenden Beratungszeiten.

Darüber hinaus können Sie über die nachfolgend angeführten Links weitere umfangreiche Tipps und Hinweise zum Thema Cybersicherheit abrufen.

- **www.polizei-beratung.de**
- **https://www.polizei.rlp.de/de/aufgaben/kriminalitaet/kriminalitaetsbekaempfung/cybercrime**
- **https://kriminalpraevention.rlp.de/de/cybersicherheit/**
- **https://www.bka.de/DE/IhreSicherheit/RichtigesVerhalten/StraftatenImInternet/internet_node.html**
- **www.bsi.bund.de**
- **https://www.sicher-im-netz.de/**

Herausgeber
Landeskriminalamt Rheinland-Pfalz
Abteilung 4 / Dezernat 47 - Cybercrime
Valenciaplatz 1-7
55118 Mainz
E-Mail: lka.cybercrime@polizei.rlp.de
Internet: www.polizei.rlp.de

[6] LINK: https://kriminalpraevention.rlp.de/de/cybersicherheit/persoenliche-beratung/