2024-06-09 Identitätsdiebstahl

Meistens eine mittlere bis größere Katastrophe für die Betroffenen. Die Möglichkeiten eines Missbrauchs sind sehr viel größer als gedacht und die Dunkelziffer ist recht hoch. Meistens wird so ein Fall erst sehr spät erkannt und es ist nur noch eine Schadensbegrenzung möglich. Ein Überblick sowie vorbeugende Maßnahmen und Reaktionen sind sinnvoll. (JDH)

Im Internet werden bereits viele Daten von Personen und Unternehmen zur Verfügung gestellt. Dies betrifft die Einrichtung von Accounts in sozialen Medien mit persönlichen Angaben sowie Pflichtangaben bei den Homepages. Damit ist schon mal ein guter Fundus vorhanden. Dazu kommen noch Daten bei der Registrierung für On-Line-Geschäfte oder auch bei vermeintlich kostenlosen Angeboten, z. B. bei Apps. Auch bei der Nutzung von kostenlosen Diensten (z. B. Nachrichtenportale) werden vermeintlich anonyme Daten gesammelt, die jedoch recht schnell personalisiert werden können. Die Technik macht es möglich. Bleiben noch die Hacker, die sich an schlecht gesicherten Daten bedienen. Besonders beliebt sind E-Mail-Accounts, mit denen dann auch neue Passwörter für vermeintlich sichere Accounts angefordert werden können.
Diese Daten reichen aus, um sich im Internet als jemand anderes auszugeben. Damit können Bankgeschäfte, Warengeschäfte und auch soziale Beiträge (Postings) durchgeführt werden. Somit ist dann der digitale Identitätsdiebstahl perfekt. Das fällt jedoch erst auf, wenn die Daten tatsächlich missbraucht wurden. Entweder kann man sich nicht mehr in seinem Account einloggen (Passwort wurde geändert) oder man erhält unbekannte Zahlungsaufforderungen oder es sind merkwürdige Buchungen auf dem eigenen Bankkonto. Noch schlimmer ist es bei Unternehmen, die z. B. Beschwerden über ausbleibende Lieferungen erhalten, jedoch selber keinen On-Line-Shop haben. Da hat dann jemand einen On-Line-Shop angelegt, der einfach die falschen Daten verwendet, aber nichts liefert. Persönlich erhält man somit Rechnungen über gelieferte Waren, die man nicht bestellt, aber jemand anderes, z. B. über eine Paketstation, erhalten hat. Weitere Hinweise sind Nachrichten im eigenen Postfach, die man selber nicht verfasst hat oder Anfragen von Bekannten, die merkwürdige Nachrichten erhalten haben, von denen man nichts weiß.

Vorbeugung

- Betriebssystem, Browserversion, Firewall und Anti-Viren-Software der Geräte stets auf dem neuesten Stand halten
- Bei nicht mehr unterstützter Software (auch Betriebssystem) auf neue Versionen wechseln
- Regelmäßige Datensicherungen auf externe Datenträger – nicht ständig mit den Geräten verbunden
- Beim Zugriff auf das Internet nur mit Benutzerkonto mit eingeschränkten Rechten, nicht als Administrator
- Konsequente Verwendung von starken Passwörtern
- Programme nur aus vertrauenswürdigen Quellen herunterladen (Original-Anbieter)
- Vor Programminstallation eine Überprüfung mittels Anti-Viren-Software durchführen
- Anhänge und Links nur dann öffnen, wenn diese eindeutig sicher sind
- Im Internet so wenig wie möglich persönliche Daten angeben (Nur Pflichtfelder)
- Bei kostenlosen Produkten mit Registrierung abwägen, die Bezahlung erfolgt mit Daten
- Nur falls unbedingt notwendig eine Registrierung durchführen
- Bei der Kontaktaufnahme durch (vermeintliche) Bekannte alternativ nachfragen
- Keine unbekannten Datenträger verwenden
- Keine wichtigen Transaktionen über öffentliche Hotspots
- Bankgeschäfte nur mit einer Zwei-Faktor-Authentifikation

Reaktion

Je nachdem, welches Problem aufgetreten ist, können Maßnahmen ergriffen werden um den Identitätsdiebstahl zu beseitigen oder die Auswirkungen zu reduzieren. Ein offenes Vorgehen ist dabei die bessere Wahl, ein Verheimlichen kann zu noch größeren Problemen führen.

- Prüfen, welche On-Line-Konten betroffen sind
- Prüfen, welche On-Line-Konten betroffen sein könnten
- Betroffene On-Line Konten
    - Passwörter zurücksetzen und neu vergeben oder
    - Konto-Anbieter informieren und den Account sperren lassen
- Bei nicht betroffenen Konten, aber gleichem Passwort, ebenfalls das Passwort ändern
- Eigene Kontakte über die Probleme informieren
- Umstellung der Zugänge auf Zwei-Faktor-Authentifizierung
- Anzeige bei der zuständigen Strafverfolgungsbehörde stellen
- Bei einer eigenen Homepage direkt auf der Startseite informieren
- Bei Mahnungen prüfen, ob diese Fake sind oder tatsächlich (aber fälschlicherweise) existieren
    - Mahnungen per Brief sind meistens leider „echt“
    - Mahnungen per E-Mail sind meistens „fake“
- Zu guter Letzt einen Anwalt hinzuziehen

Eine einfache, standardisierte Lösung für dieses Problem gibt es nicht. Es kann auch jederzeit jeden treffen, deswegen sollte besser in die Vorsorge investiert werden. Gerade für kleine Unternehmen mit eigener Homepage und/oder Auftritt in den sozialen Medien mit dem damit verbundenen Pflichtangaben wäre ein Leitfaden für den Umgang mit solch einem Problem sinnvoll.

Jochen D. Hohenwald