

Erste Hilfe – Identitätsmanagement

Jede missbräuchliche Nutzung Ihrer persönlichen Daten, also von Teilen einer Ihrer Identitäten, wird als Identitätsdiebstahl bezeichnet. Das kann zur Bildung falscher beziehungsweise verfälschter (Nutzer-)Profile führen; das kann Ihnen wirtschaftlichen Schaden zufügen (etwa durch Missbrauch von Kreditkartendaten) oder rufschädigend sein. Dies gilt insbesondere bei Diensten im Internet, beispielsweise beim Einsatz von Rabattkarten oder in Fällen, da gestohlene Identitäten genutzt werden, um Sozialleistungen zu erschleichen.

Durch Identitätsdiebstahl kann im Zweifel auf eine Vielzahl wichtiger Daten zugegriffen werden, die niemanden etwas angehen. Sie sollten immer auf der Hut sein vor Versuchen Anderer, sich Ihre Identitäten anzueignen. Das schließt Ihre eigene Vorsorge ein – so sollten Sie nie in E-Mails etwa Zugangsdaten für Ihr Konto übermitteln; nicht nur bei Web-Mail-Anbietern können die leicht in falsche Hände geraten. Andererseits könnten Ihnen unter falschem Absender Mails zugesandt werden, die von Ihrer Bank zu kommen scheinen; vielleicht werden Sie dort unter irgendeinem Vorwand dazu aufgefordert, auf einen in der Mail enthaltenen Link zu klicken: Das führt Sie dann beispielsweise auf eine der Original-Internet-Präsenz Ihrer Bank täuschend echt nachempfundenen Internet-Seite, wo Ihre Zugangsdaten zum Online-Banking samt Bestätigung mit einer gültigen TAN gefordert werden (Phishing-Attacke). Nähere Informationen hierzu finden unter http://www.datenschutz-bremen.de/newmedia/online_banking.php

Wenn Sie schon "Identitäten" nutzen wollen oder müssen, dann wählen Sie möglichst viele verschiedene, von einander unabhängige. So ist es durchaus üblich, mehrere Mailadressen (etwa eine private für den Mailaustausch mit Freunden und eine für Konsum-Zwecke) zu unterschiedlichen Zwecken einzurichten. Geben Sie Dritten niemals Passwörter, Benutzernamen oder Zugangsdaten zu Mail- oder Bankkonten bekannt. Geben Sie Identitäts-Daten wie beispielsweise Ihre Krankenversicherungsnummer allenfalls an befugte Empfänger: im Zweifel sollten Sie sich an geeigneter Stelle rückversichern, ob diese Befugnis tatsächlich besteht.

Sichern Sie Ihr eigenes Computersystem möglichst umfangreich mit geeigneten technischen Mitteln gegen missbräuchliche Nutzung und damit den möglichen Diebstahl Ihrer Identitäten; falls Sie selbst glauben, das nicht leisten zu können, holen Sie sich Hilfe von vertrauenswürdiger Seite, ob von Freunden, Kollegen oder einschlägigen Firmen: Schützen Sie Ihren Computer gegen unerwünschtes Eindringen mit einer "Firewall", halten Sie Ihren Virens Scanner stets aktuell, installieren Sie immer alle verfügbaren Sicherheitsupdates zum Betriebssystem und Ihren sonstigen genutzten Programmen. Speichern Sie niemals Zugangsdaten (Benutzernamen oder Passwörter) auf Ihrem Computer. Weiterführende Informationen bieten wir Ihnen unter <http://www.datenschutz-bremen.de/mainsv.php>

Und schließlich: Seien Sie kritisch gegenüber allen Berichten und Versuchen, die darauf zielen, Ihre vielen Identitäten zusammenzufassen, zu zentralisieren. Ob Ihnen eine gemeinsame Rabattkarte von mehreren Anbietern nahegelegt oder eine zentrale Steuernummer zugeordnet wird: Hinterfragen Sie derartige Bestrebungen und suchen Sie über diese und ähnliche Fragen die Diskussion mit Interessenvertretern (wie zum Beispiel Bürgerinitiativen) oder den Kreis-, Land- oder Bundestagsabgeordneten Ihres Wahlkreises.