In deinem Namen

Nicht nur die Geheimdienste greifen nach Daten. Digitaler Identitätsdiebstahl belastet die Opfer und macht umfassenden E-Commerce zur Hochrisikoaktion

Joachim Jakobs

Im Juni 2015 berichtete der Journalist Julius Stucke von seinen persönlichen Erfahrungen mit dem Phänomen »Identitätsdiebstahl«: Ein Dritter habe in seinem Namen eine Sitzecke bestellt und nicht bezahlt. Daraufhin habe sich ein Anwalt bei ihm gemeldet und eine Gesamtforderung einschließlich Gebühren in Höhe von 800 Euro eintreiben wollen. Wie sich die Betrüger dem Verkäufer gegenüber als Stucke ausgewiesen haben, ist dem Journalisten nicht bekannt. Die Händler glauben dem Besteller nur allzu gern und begnügen sich oft schon mit dem Geburtsdatum. Wenn dann nicht bezahlt wird, ermittelt man den mutmaßlichen Besteller per Schufa und drängt ihn zunächst per Rechnung, dann wahlweise per Inkassounternehmen oder Anwalt zur Zahlung. Parallel geht der Missbrauch von Stuckes Identität weiter: Kreditverträge, Kfz-Teile, Pay-TV-Vertrag, Telekommunikationsvertrag. Dadurch kann die Kreditwürdigkeit des Bestohlenen leiden – die tatsächlichen Dienstleister wie etwa Banken, Versicherungen oder der Vermieter könnten mit der Kündigung der tatsächlichen Verträge drohen und neue Geschäfte erst gar nicht zustande kommen. Inkassounternehmen sollen demnach mit der Pfändung von Konto und Gehalt drohen. Auch die Schufa hält sich für unschuldig. Sie stützt sich – ihrer Meinung nach – bei ihren Berechnungen ja nur auf die Hinweise Dritter.

Das Ganze ist jedoch noch steigerungsfähig: Der Gesetzgeber will die Geldwäsche bekämpfen und verpflichtet zahlreiche Berufe wie Anwälte, Steuerberater oder Banken, ihre Klientel zu identifizieren. Ein Immobilienmakler benennt in solchen Fällen dann nicht nur jene, die später tatsächlich mieten oder kaufen, sondern sämtliche Interessenten, die das Objekt ansehen. Nicht alle »Dienstverpflichteten« sind in der Lage, die Ausweise sicher zu verwahren. Davon berichtete eine Frau aus Berlin dem *MDR*-Magazin »Fakt« im Januar 2014: Bei ihrer Wohnungssuche interessierte sie sich für die Angebote von drei Maklern. Einem davon wurde nach Vermutung der Staatsanwaltschaft die Ausweiskopie gestohlen. Die Betroffene sagte: »Es ist ein Ebay-Account auf mich angemeldet worden. Es sind Paypal-Konten auf meinen Namen angemeldet worden, Kreditkarten bestellt worden. Es sind Konten eröffnet worden. Es wurde eingekauft in meinem Namen, und die Liste könnte ich unendlich fortsetzen.«
Martin Steltner von der Berliner Staatsanwaltschaft erklärte vor der »Fakt«-Kamera, seine Behörde habe gegen die Immobilienmakler wegen der gestohlenen Ausweiskopie ermittelt. Die Vermittler wissen von Ermittlungen nichts. Am Ende blieb das Opfer auf sich allein gestellt. Der Berliner Beauftragte für Datenschutz, Alexander Dix, empfahl ihr im Februar 2014, Akteneinsicht zu beantragen, notfalls auch mit anwaltlicher Unterstützung. Unklar bleibt in jedem Fall, wieso sich Personen identifizieren müssen, die sich lediglich erst einmal für eine Wohnung interessieren. Das scheint dem Gebot der Datensparsamkeit zu widersprechen.

Für den elektronischen Identitätsmissbrauch sind die Daten aus dem Ausweis ausreichend. Drogenhändler

und Terroristen agieren in dieser Hinsicht materiell: sie bevorzugen für ihre Aktivitäten Ausweise in physischer Form. Mit Hilfe der entwendeten Daten sollen sich Duplikate der Dokumente herstellen lassen. Gestohlene Ausweisdaten sind wie ein Damoklesschwert, das den rechtmäßigen Inhaber bei jedem Grenzübertritt treffen kann.

Deshalb bringt jede Information, jedes Passwort, jede PIN und jede Zugangsberechtigung offenbar Bares: Das Geburtsdatum einer Person ist Kriminellen drei US-Dollar wert, Kreditkartendaten 1,50 Dollar und der Mädchenname einer Frau sechs Dollar. Eine ganze Krankenakte kostet schon 50 Dollar.

Bürger, Kunden und Patienten sind also von zwei Seiten bedroht, wenn sie ihre Daten Behörden, Unternehmen oder Ärzten anvertrauen: Die einen sind offensichtlich der Ansicht, ihre Klienten haben »nichts zu verbergen«. Im Februar 2015 wurden Röntgenunterlagen des Klinikums Weilheim im 60 Kilometer entfernten München »sackweise« auf der Straße gefunden.

Die anderen lassen keine Gelegenheit aus, um Beute zu machen: Mal werden Patientenakten in Papierform, mal auf Festplatte von den Lkw gestohlen. Nicht einmal Entsorgtes ist vor Plünderung gefeit – eine Detektei, die A Plus Detective GmbH, warnt auf ihrer Webseite: »Die Diebe wühlen im Müll fremder Leute, um an Papiere mit Ihren persönlichen Informationen zu kommen.«

Da kann man nur hoffen, dass das Papier geschreddert wurde, bevor es in die Tonne kam. Doch auch das Schreddern will gelernt sein: Die analogen Papierstreifen lassen sich digitalisieren und anschließend wieder zusammensetzen. Ein digitaler Puzzledienst ist unter unshred.com zum Einführungspreis ab 90 US-Dollar zu buchen.

Um diesen Leuten die Suppe zu versalzen, muss die Qualität der Entsorgung erhöht werden – oder besser: Die Papierschnipsel müssen so klein sein, dass die Software keine Schnittkanten und keine Schatten auf den Fetzen mehr erkennt. Wie klein »so klein« ist, bleibt unklar: 2011 haben Wissenschaftler aus San Francisco einen Wettbewerb gewonnen, bei dem fünf Dokumente aus 10.000 Papierfetzen wieder zusammenzusetzen waren.

Der Autor hat das Buch »Vernetzte Gesellschaft. Vernetzte Bedrohungen – Wie uns die künstliche Intelligenz herausfordert« geschrieben. Erschienen im September im Cividale-Verlag

---

http://www.jungewelt.de/2015/11-18/038.php