Sachstand

„Identitätsdiebstahl“ im Internet

Überblick und rechtliche Implikationen

[redacted]

© 2014 Deutscher Bundestag

„Identitätsdiebstahl“ im Internet
Überblick und rechtliche Implikationen

Verfasser: [redacted]
Aktenzeichen: WD 7 - 3000 - 183/14
Abschluss der Arbeit: 16. September 2014
Fachbereich: WD 7: Zivil-, Straf- und Verfahrensrecht, Umweltschutzrecht, Verkehr, Bau- und Stadtentwicklung
Telefon: [redacted]

Ausarbeitungen und andere Informationsangebote der Wissenschaftlichen Dienste geben nicht die Auffassung des Deutschen Bundestages, eines seiner Organe oder der Bundestagsverwaltung wieder. Vielmehr liegen sie in der fachlichen Verantwortung der Verfasserinnen und Verfasser sowie der Fachbereichsleitung. Der Deutsche Bundestag behält sich die Rechte der Veröffentlichung und Verbreitung vor. Beides bedarf der Zustimmung der Leitung der Abteilung W, Platz der Republik 1, 11011 Berlin.

Inhaltsverzeichnis

1. Einleitung

Das Phänomen des „Identitätsdiebstahls im Internet“ erlangt aufgrund immer wieder erfolgender groß angelegter „Hackerangriffe“ bzw. „Datenschutzpannen“ zunehmende Aufmerksamkeit.[1] Nachfolgend wird der aktuelle Erkenntnisstand zum Identitätsdiebstahl[2] summarisch dargestellt.

2. Wie hoch ist aktuell die Anzahl an Identitätsdiebstählen in Deutschland? Mit welcher Dunkelziffer ist zu rechnen? Wie ist die Entwicklung im Zeitverlauf der letzten Jahre?

Informationen über aktuelle Vorkommnisse aus dem Bereich „Cyber-Sicherheit“ werden regelmäßig vom Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht. Lage-Informationen des BSI zum Datenabfluss bzw. Identitätsdiebstahl durch Schadsoftware-Infektionen in Deutschland weisen für den Zeitraum von April 2012 bis Juni 2013 folgende Zahlen aus:

Jahr	**Monat**	**Gesamtzahl infizierter Systeme**
2012	April	33.408
2012	Mai	64.100
2012	Juni	55.892
2012	Juli	254.056
2012	August	231.052
2012	September	82.609
2012	Oktober	73.458
2012	November	74.439

1 Vgl. Heckmann, jurisPR-ITR 10/2014 Anm 1 (im Bundestags-Intranet abrufbar unter http://www.juris.de/jportal/portal/t/fxz/page/jurisw.psml?doc.hl=1&doc.id=jpr-NLI-TEDT001014&documentnumber=1&numberofresults=6&showdoccase=1&doc.part=S&paramfromHL=true#focuspoint – Stand dieser und sämtlicher nachfolgenden Online-Quellen: 15. September 2014).

2 Unter „Identitätsdiebstahl“ wird vorliegend im Anschluss an Borges/Schwenk/Stuckenberg/Wegener das unbefugte Sichverschaffen einer Identität – also einer Menge an Daten, durch die eine andere Person in einem bestimmten Zusammenhang eindeutig bezeichnet wird – verstanden (Borges/Schwenk/Stuckenberg/Wegener, Identitätsdiebstahl und Identitätsmissbrauch im Internet – Rechtliche und technische Aspekte, 2011, S. 11 (im Bundestags-Intranet abrufbar unter http://link.springer.com/book/10.1007%2F978-3-642-15833-9#section=845253&page=1).

2012	Dezember	97.667
2013	Januar	135.510
2013	Februar	77.340
2013	März	39.047
2013	April	35.476
2013	Mai	36.867
2013	Juni	32.529

Das BSI weist darauf hin, dass die o.g. Zahlen nur einen Ausschnitt des Problems in Deutschland zeigen und dass die Dunkelziffer vermutlich „sehr viel höher“ sei.[3]

3. Nach welchen Gesetzen wird Identitätsdiebstahl bislang in Deutschland geahndet?

In Betracht kommen, wenn unkörperliche Informationen erlangt werden, eine Strafbarkeit wegen Ausspähen von Daten (§ 202a StGB), Abfangen von Daten (§ 202b StGB), Vorbereiten des Ausspähens und Abfangens von Daten (§ 202c StGB), Datenveränderung (§ 303a StGB).[4] Wird zugleich ein Datenträger erlangt, kommen darüber hinaus, je nach den Umständen des Einzelfalls, Diebstahl (§ 242 StGB), Unterschlagung (§ 246 StGB), Betrug (§ 263 StGB), Erpressung (§ 253), Raub (§ 249 StGB) und Räuberische Erpressung (§ 255 StGB) in Betracht.[5]

4. Wie ist die Gesetzeslage in anderen europäischen Ländern?

Hierzu vgl. die Zusammenstellung bei Borges/Schwenk/Stuckenberg/Wegener, Kapitel 6 Ziff. III

Anlage.

5. Wie wird ein gesonderter Straftatbestand von Experten beurteilt?

Im Schrifttum wird unter anderem konstatiert, dass nach geltendem Recht keine Strafbarkeitslücken bestünden, so dass insoweit kein Bedarf für eine Gesetzesänderung bestünde.[6] Zwar wird

3 BSI, Lageinformation Datenabfluss durch Schadsoftware-Infektionen in Deutschland, April 2012, S. 2.

4 Borges/Schwenk/Stuckenberg/Wegener a.a.O. S. 202.

5 Borges/Schwenk/Stuckenberg/Wegener a.a.O. S. 202.

6 Borges/Schwenk/Stuckenberg/Wegener a.a.O. S. 373.

konzediert, ein gesonderter Straftatbestand könne dazu dienen, den spezifischen Unrechtscharakter hervorzuheben – ein Bedürfnis hierfür sei jedoch derzeit ebenfalls nicht gegeben.[7]

Auf internationaler Ebene befassen sich sowohl die Europäische Union als auch die Vereinten Nationen mit der Thematik und haben dazu Studien veröffentlicht.[8]

6. Zu welchen Zwecken werden die gestohlenen Identitäten eingesetzt?

In der Literatur werden genannt: Spaßbestellungen im Online-Handel, Kreditkartenmissbrauch, Versenden von SPAM-E-Mails, Zugriff auf fremde Online-Banking-Konten.[9] Vermehrt stellen die Identitäten offenbar auch selbst einen Wert dar, der sie der illegalen wirtschaftlichen Verwertung zugänglich macht.[10]

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

Einschlägige empirische Informationen speziell zum Phänomen Identitätsdiebstahl liegen nicht vor. Laut Bundeskriminalamt lag der Schaden im Bereich der Cyberkriminalität 2013 bei 42,6 Mio. Euro.[11]

8. Welche Ansätze werden seitens der Sicherheitsbehörden zur Bekämpfung des Identitätsdiebstahls verfolgt bzw. empfohlen?

Das BSI umschreibt die von ihm gewählten grundsätzlichen Ansätze wie folgt:

„Der Schutz des deutschen Anteils am Cyber-Raum und das Vorhandensein möglichst widerstandsfähiger Infrastrukturen, sind wesentliche Ziele deutscher Politik. So wurde 2009 mit Blick auf die Bundesverwaltung mit der Novellierung des BSI-Gesetzes eine erste, an die neue Bedrohungslage angepasste, rechtliche Grundlage geschaffen. Die am 23. Februar 2011 im Kabinett be-

---

7 Borges/Schwenk/Stuckenberg/Wegener a.a.O. S. 373.

8 Vgl. European Commission, Directorate General for Home Affairs, Study for an Impact Assessment on a Proposal for a New Legal Framework on Identity Theft, 2012 (abrufbar unter: http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/final_report_identity_theft_11_december_2012_en.pdf) sowie die Zusammenstellung von Informationen auf der Website "UNODC Response to Identity-related Crime", abrufbar unter http://www.unodc.org/unodc/en/organized-crime/identity-related-crime.html.

9 Borges/Schwenk/Stuckenberg/Wegener a.a.O. S. 27 f.

10 Vgl. etwa Stellungnahme der Bundesregierung zum Gesetzentwurf des Bundesrates, Entwurf eines Gesetzes zur Strafbarkeit der Datenhehlerei, BT-Drs. 18/1288, S. 20.

11 Vgl. BKA, Cybercrime Bundeslagebild 2013, abrufbar unter: http://www.bka.de/nn_231576/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2013,templateId=raw,property=publicationFile.pdf/cybercrimeBundeslagebild2013.pdf.

schlossene „Cyber-Sicherheitsstrategie für Deutschland“[12] erweitert den Betrachtungsrahmen nun auch auf Bereiche außerhalb der Bundesverwaltung. Das BSI nimmt mit seinen Einrichtungen und Aktivitäten bereits zahlreiche Aufgaben zur Umsetzung der Cyber-Sicherheit in Deutschland wahr. Hierzu gehören neben dem Betrieb des Nationalen IT-Lagezentrums, der federführenden Zusammenarbeit im Nationalen Cyber-Abwehrzentrum und der Zusammenarbeit beim Schutz Kritischer Infrastrukturen auch viele weitere Aufgabenfelder aus dem Produktportfolio des BSI als zentrale IT-Sicherheitsbehörde des Bundes.“[13]

Mit einer „Cyber-Sicherheitsstrategie für Deutschland“ passe die Bundesregierung die auf Basis der Umsetzungspläne KRITIS (UP KRITIS) und Bund (UP Bund) aufgebauten Strukturen und Maßnahmen durch Vorhaben in zehn strategischen Bereichen an die Gefährdungslage an.[14] Diese Bereiche sind:[15]

- Schutz kritischer Informationsinfrastrukturen
- Sichere IT-Systeme in Deutschland
- Stärkung der IT-Sicherheit in der öffentlichen Verwaltung
- Nationales Cyber-Abwehrzentrum
- Nationaler Cybersicherheitsrat
- Wirksame Kriminalitätsbekämpfung im Cyber-Raum
- Effektives Zusammenwirken für Cyber-Sicherheit in Europa und weltweit
- Einsatz verlässlicher und vertrauenswürdiger Informationstechnologie
- Personalentwicklung der Bundesbehörden
- Instrumentarium zur Abwehr von Cyberangriffen.

---

12 http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber.pdf;jsessionid=801EB4E935B1775DFC16AE41272F5358.2_cid287?__blob=publicationFile.

13 https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Strategie/cs_Strategie_node.html;jsessionid=78E4877B33858B474B7FEF2CC302AF3E.2_cid359.

14 https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Strategie/cs_Strategie_node.html;jsessionid=78E4877B33858B474B7FEF2CC302AF3E.2_cid359.

15 Vgl. https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Strategie/cs_Strategie_node.html;jsessionid=78E4877B33858B474B7FEF2CC302AF3E.2_cid359.

Konkret veröffentlicht das BSI regelmäßig Informationen zu aktuellen Vorkommnissen im Bereich von Identitätsdiebstählen[16] und hat präventiv etwa „Mindestanforderungen zur Informationssicherheit bei eCommerce-Anbietern“ veröffentlicht.[17]

9. Welche Vorsichtsmaßnahmen werden den Bürgern empfohlen?

Seitens der Polizeibehörden werden den Bürgern folgende präventiven Maßnahmen empfohlen:

- „Setzen Sie eine Firewall und Virenschutzsoftware ein und bringen Sie diese regelmäßig auf den aktuellen Stand. Achten Sie darauf, dass Sie auch beim Betriebssystem und bei anderen von Ihnen eingesetzten Programmen (wie z.B. Adobe Reader, Flash etc.) vom Hersteller bereitgestellte Sicherheitsupdates zeitnah installieren oder nutzen Sie automatische Update-Dienste.

- Öffnen Sie niemals ungeprüft Dateianhänge von E-Mails. Ganz gleich, ob es sich um scheinbar ungefährliche Dateien wie Bilder, Dokumente oder sonstige Dateien handelt. Wenn Sie unsicher sind, fragen Sie sicherheitshalber beim Absender nach.

- Oft verraten sich virenbehaftete E-Mails durch einen Betreff, der den Adressaten neugierig machen soll (z. B. mit Begriffen aus dem Erotikbereich, zu aktuellen Promi-Skandalen oder Katastrophen).

- Seien Sie misstrauisch, wenn Sie E-Mails von angeblichen Bekannten ohne oder mit fremdsprachigem Betreff erhalten. Wenn Sie solche E-Mails unaufgefordert erhalten, sollten Sie diese sofort löschen.

- Seien Sie besonders kritisch bei ausführbaren Programm-Dateien mit den Endungen .exe, aber auch .bat, .com oder .vbs und insbesondere bei doppelten Dateiendungen wie .doc.exe. Damit der Dateityp zu sehen ist, sollten Sie die Standardkonfiguration ihres Rechners entsprechend ändern (im Windows-Explorer unter „Extras - Ordneroptionen - Ansicht - Erweiterte Einstellungen - Dateien und Ordner“ das Häkchen vor „Erweiterungen bei bekannten Dateitypen ausblenden“ entfernen).

- Stellen Sie die Sicherheitseinstellungen Ihres E-Mail-Programms so ein, dass kein Script automatisch ausgeführt wird.

- Kontaktieren Sie Ihre Bank oder Ihren Geschäftspartner, wenn Sie befürchten, dass Sie einem Phishing-Angriff zum Opfer gefallen sind! Die für Sicherheitsfragen zuständigen Mit-

---

16 Vgl. etwa https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Neuer_Fall_von_Identitaetsdiebstahl_07042014.html oder https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Milliardenfacher_Datendiebstahl_06082014.html.

17 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Mindestanforderungen-eCommerce-Anbieter.pdf?__blob=publicationFile.

arbeiter können den Vorfall verfolgen und prüfen, ob Schaden entstanden ist. Falls tatsächlich bereits Summen unberechtigt überwiesen worden sind, so wenden Sie sich bitte umgehend an die Polizei.

– Obgleich klassisches Phishing immer weniger zu beobachten ist: Vermeiden Sie es, auf Links in unaufgefordert zugesandten E-Mails zu klicken. Diese können zu gefälschten oder infizierten Webseiten führen. Aktivieren Sie den Phishing-Schutz in Ihrem Webbrowser.

– Kreditinstitute fordern grundsätzlich keine vertraulichen Daten per E-Mail oder per Telefon von Ihnen an. Auch der Kontostand sowie Kontobewegungen sollten regelmäßig kontrolliert werden. So kann man schnell reagieren, falls ungewollte Transaktionen stattgefunden haben.“[18]

[redacted]

18 http://www.polizei-beratung.de/presse/646-betrueger-setzen-schadsoftware-fuer-datendiebstahl-ein.html.