

Tatort Internet: Kriminalität verursacht Bürgern Schäden in Milliardenhöhe

Von Johannes Rieckmann, Martina Kraus

Internetkriminalität kann für die Betroffenen erhebliche Kosten zur Folge haben. Bisherige Ansätze der Quantifizierung konzentrierten sich meist auf Schäden für Unternehmen. Offizielle Angaben zu Schäden für Privatpersonen beruhen in erster Linie auf den polizeilich erfassten Fällen, dadurch wird die tatsächliche Belastung der Bürger aber nicht annähernd wiedergegeben. In der vorliegenden Untersuchung, die auf einer breit angelegten Befragung beruht, wird der finanzielle Schaden für Privatpersonen abgeschätzt. Er beläuft sich in vier wichtigen Bereichen der Internetkriminalität – Phishing, Identitätsbetrug, Waren- und Dienstleistungsbetrug und Schadsoftware – jährlich auf insgesamt 3,4 Milliarden Euro, dies entspricht 0,1 Prozent des deutschen Bruttoinlandsprodukts.

Der Gebrauch des Internets ist alltäglich und unverzichtbar geworden. Aus einer vom DIW Berlin durchgeführten Befragung¹ geht hervor, dass 72 Prozent der Bevölkerung das Internet täglich, zumindest aber mehrmals in der Woche oder im Monat nutzen. Nur noch gut ein Viertel der Bürger gibt an, nie oder sehr selten im Internet aktiv zu sein. Durch seine Rolle im Alltag kommt dem Internet auch als Kriminalitätsfeld mehr und mehr Bedeutung zu. Bisherige Studien der Kriminalitätsforschung weisen zwar auf ein großes Dunkelfeld bei Internetkriminalität hin, vermessen dieses unbekanntes Gebiet aber nicht.² Diese Datenlücke versucht ein Teilbereich des WISIND-Projektes zu schließen. In diesem Bericht werden vier Kategorien der Internetkriminalität auf ihre Bedeutung untersucht. Diese umfassen Phishing³, Identitätsbetrug, Waren- und Dienstleistungsbetrug sowie Angriffe mit Schadsoftware. Zwischen Juli und September 2014 wurden dafür gut 12 000 Personen in Deutschland telefonisch zu ihrer Erfahrung mit und ihrer Wahrnehmung von Internetkriminalität

1 Die Befragung wurde im Rahmen des Forschungsprojekts *Ein Wirtschaftswissenschaftlicher Sicherheitsindikator für Deutschland (WISIND)* durchgeführt. Das Projekt wird vom Bundesministerium für Bildung und Forschung in der Förderlinie „Gesellschaftliche Dimensionen der Sicherheitsforschung“ ermöglicht. Die Konzeptionierung des WISIND-Projektes sowie die Erhebung und Analyse der WISIND-eigenen Daten sind in Zusammenarbeit mit Martin Kroh, Mathias Bug, Kristina Meier, Eric van Um und Nina Wald sowie den Mitarbeitern des Brandenburgischen Instituts für Gesellschaft und Sicherheit (BIGS) entstanden. Die Autoren danken darüber hinaus Enrique Fernandez, Jan-Lucas Schanze und Bartosz Walenda für ihre Unterstützung während dieser Prozesse.

2 Siehe zum Beispiel European Social Survey (2012): Main Questionnaire. www.europeansocialsurvey.org/docs/round6/fieldwork/source/ESS6_source_main_questionnaire.pdf, Zugriff am 02.03.2015; Europäische Kommission (2014): Special Eurobarometer 423. 41-78, ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf, Zugriff am 02.03.2015; Baier, D. et al. (2011): Kriminalitätsfurcht, Strafbedürfnisse und wahrgenommene Kriminalitätsentwicklung. 133-139, www.kfn.de/versions/kfn/assets/fob117.pdf, Zugriff am 20.02.2015; Birkel, C. et al. (2014): Der Deutsche Viktimisierungssurvey. 27-30, www.mpicc.de/files/pdf3/a7_2014_Viktimisierungssurvey_2012.pdf, Zugriff am 20.02.2015; LKA Niedersachsen (2013): Befragung zu Sicherheit und Kriminalität in Niedersachsen. 19-25, www.mi.niedersachsen.de/download/82334, Zugriff am 26.02.2015.

3 Unter Phishing versteht man Missbrauch von Bankkonten oder Kreditkarten mittels über das Internet betrügerisch erlangter geheimer Passwörter.

befragt. Aufgrund der Größe und Repräsentativität der Befragung erlaubt diese eine genauere Einschätzung des Dunkelfeldes, sowohl bezüglich der Fallzahlen, das heißt der Viktimisierung durch Internetkriminalität, als auch der daraus entstehenden finanziellen Kosten.

Internetkriminalität ist bislang überwiegend unsichtbar

Die polizeiliche Kriminalstatistik wird jährlich vom Bundeskriminalamt veröffentlicht und liefert eine Übersicht zu den Fallzahlen in einzelnen Deliktgruppen.⁴ Allerdings tauchen nur diejenigen Fälle in der Statistik auf, die bei der Polizei zur Anzeige gebracht oder von dieser aufgrund eigener Ermittlungstätigkeit entdeckt werden (das so genannte Hellfeld). Relativ zuverlässig angezeigt werden Delikte, die als versicherbar gelten.⁵ Auf der anderen Seite gibt es Kriminalitätsbereiche, bei denen viele Taten gar nicht zur Anzeige gebracht werden. Bei Internetkriminalität ist das Dunkelfeld besonders groß, wie auch dieser Bericht bestätigt.

Auf der Basis der oben genannten Befragung können eine auch das Dunkelfeld umfassende Fallzahl und der daraus entstandene Gesamtschaden errechnet werden. Solche Schadensschätzungen gibt es bereits für den gewerblichen,⁶ nicht jedoch für den privaten Bereich.

Die auf der Befragung basierenden Hochrechnungen bieten Zahlen für den Zeitraum von Anfang 2012 bis September 2014, die anschließend in durchschnittliche Jahreswerte umgerechnet werden.⁷ In der Untersuchung wird nach den oben genannten vier Deliktformen differenziert. Für diese ergibt sich auf Basis der Repräsentativbefragung ein Gesamtumfang von mehr als 14,7 Millionen Fällen pro Jahr. Nach der polizeilichen Kriminalstatistik belief sich die Zahl der Delikte im Bereich Information und Kommunikation im Jahr 2013 dagegen auf lediglich 64 426 Fälle.⁸

⁴ Bundesministerium des Innern (2013): Polizeiliche Kriminalstatistik. 16-23. www.bmi.bund.de/SharedDocs/Downloads/DE/Nachrichten/Pressemitteilungen/2014/06/PKS2013.pdf?__blob=publicationFile, Zugriff am 20.02.2015. Für eine kritische Betrachtung siehe Sessar, K. (2012): Kriminalitätswirklichkeit im Licht des Dunkelfeldes. In: Festschrift für Wolfgang Heinz, Baden-Baden, 265; Bug, M., Meier, K. (2015), a. a. O.

⁵ Für eine Auseinandersetzung zu Hell- und Dunkelfeld siehe Heinz, W. (2006): Zum Stand der Dunkelfeldforschung in Deutschland. In: Oberfell-Fuchs, J., Brandenstein, M. (Hrsg.): Nationale und internationale Entwicklungen in der Kriminologie. Festschrift für Helmut Kury zum 65. Geburtstag, Frankfurt a. M., 242.

⁶ KPMG schätzt die Schäden bei Unternehmen für 2012 und 2014 auf insgesamt 54 Milliarden Euro, Frankfurter Allgemeine Zeitung, 11.03.2015; siehe auch www.kpmg.com/DE/de/Documents/e-crime-studie-2015.pdf, Zugriff am 11.03.2015.

⁷ Da das Jahr 2014 von der Befragung nur zu zwei Dritteln abgedeckt wird, werden für die Berechnung von Jahreswerten die Zahlen für den Gesamtzeitraum nicht durch drei, sondern durch 2 2/3 dividiert.

⁸ Siehe hierzu BKA (2013): Bundeslagebild Cybercrime. 5.

Schäden lassen sich in Geldwerten ausdrücken

Die Schwere von bestimmten Delikten kann anhand des Schadens an Leib und Leben, der Einschränkung der Lebensqualität und seelischer Belastung oder auch durch die daraus entstehenden finanziellen Kosten beurteilt werden. Letztere Methode wird häufig in der Wirtschafts-, aber auch in der Kriminalitätsforschung benutzt.⁹ Im Bereich Internetkriminalität fällt der finanzielle Aspekt mutmaßlich weit mehr ins Gewicht als andere Schadensdimensionen, und er lässt sich quantitativ erfassen.

Die Kosten im Bereich Internetkriminalität lassen sich in fünf Kategorien einordnen: Erstens sind antizipierende Kosten zu berücksichtigen, das heißt Schutzausgaben (etwa für Antivirus-Software oder Versicherungsbeiträge), die mögliche zukünftige Schäden durch Internetkriminalität verhindern oder abfedern sollen. Zweitens gibt es unmittelbare Kosten, die durch Internetkriminalität entstehen. Diese können Verluste wie unrechtmäßige Kontobelastungen oder erpresste Gelder umfassen. Drittens spricht man von Kompensationskosten, die als Reaktion auf Internetkriminalität entstehen (zum Beispiel Entschädigung von Opfern). Nicht zu vernachlässigen sind viertens auch mittelbare Verluste wie reduzierte Wettbewerbsfähigkeit im Fall von Diebstahl geistigen Eigentums. Diese spielen in diesem Bericht keine Rolle, da sich die Untersuchung nicht auf Unternehmen, sondern auf Individuen bezieht. Schließlich spielen fünftens Kosten im weiteren Sinn eine Rolle, die zum Beispiel Reputationsverluste oder Vertrauensverlust in internetbasierte Transaktionen umfassen.¹⁰

Bisherige Studien zu Internetkriminalität greifen in Ermangelung von Daten zu konkreten Schadenssummen oft auf ökonomische Schätzverfahren zurück.¹¹

⁹ Bug, M., Meier, K. (2014): Herausforderungen bei der Messung von Kriminalität. DIW Roundup 24, 4; siehe auch Miller T., Cohen, M. A., Wiersema, B. (1996): Victim Costs and Consequences: A New Look. Washington, D.C., U.S. Department of Justice, purl.access.gpo.gov/GPO/LPS91581, Zugriff am 12.06.2014, Office of Justice Programs, National Institute of Justice; sowie für den europäischen Raum Entorf, H., Spengler, H. (2002): Crime in Europe: Causes and Consequences. Und für Deutschland Entorf, H., Sieger, P. (2010): Unzureichende Bildung: Folgekosten durch Kriminalität. Research Report on behalf of Bertelsmann Stiftung, 11/2010, www.wiwi.unifrakfurt.de/fileadmin/user_upload/dateien_abteilungen/abt_ewf/LS_Entorf/doc/Entorf/Abschlussbericht.pdf, Zugriff am 12.06.2014.

¹⁰ Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., Savage, S. (2013): Measuring the Cost of Cybercrime. In: Böhme, R. (Hrsg.): The Economics of Information Security and Privacy. Heidelberg, weis2012.econinfocsec.org/papers/Anderson_WEIS2012.pdf, Zugriff am 23.02.2015.

¹¹ Während das Bundesamt für Sicherheit in der Informationstechnik (BSI) die monetäre Bewertung der Fälle von Internetkriminalität in seinen Publikationen bislang in der Regel vermeidet und eher Fallzahlen schätzt, für 2010 beispielsweise 1,107 Millionen Phishing-Fälle, siehe BSI (2011): Lagebericht IT-Sicherheit in Deutschland. 23, nennt das Bundeskriminalamt

Der Fokus vieler Umfragen liegt auf den finanziellen Schäden für Unternehmen oder Staaten,¹² nicht aber auf den Kosten für die von Internetkriminalität betroffene Bevölkerung direkt.¹³ Im Rahmen der vorliegenden Studie wurden dagegen die den Bürgern entstandenen finanziellen Schäden konkret abgefragt (Kasten). Dies ermöglicht eine genauere Berechnung der Kosten, die durch Internetkriminalität in Deutschland von 2012 bis 2014 entstanden sind. Hierbei liegt das Augenmerk auf den unmittelbaren Kosten. Die oben genannten Kategorien der antizipierenden bzw. mittelbaren Kosten können mangels entsprechender Daten nicht einbezogen werden.

Jeder Fünfte Opfer von Internetkriminalität

Von den 11 877 Befragten¹⁴ gaben 2 580 (gut ein Fünftel)¹⁵ an, zwischen Anfang 2012 und Spätsommer 2014 Opfer von Internetkriminalität geworden zu sein. In 1 439 Fällen waren dieselben Befragten sogar mehrfach betroffen. Die Fallzahlen sind daher um einiges höher als die Zahl der Opfer. Von den sich aus der Hochrechnung ergebenden 14,7 Millionen jährlichen Fällen von

(BKA) Geldsummen: Laut der Behörde belief sich der Schaden im Bereich Computerbetrug und Betrug mit Zugangsdaten für das Jahr 2013 in Deutschland auf rund 42,6 Millionen Euro (2012 auf 42,5 Millionen Euro) und im Bereich Phishing auf 16,4 Millionen Euro (2012 auf 13,8 Millionen Euro), siehe BKA (2013): Bundeslagebild Cybercrime. 7 f. Die Global Fraud Study von 2012 untersucht 1 388 Fälle weltweit und schätzt den Median aller Verluste durch Betrug auf umgerechnet 125 000 Euro, siehe ACFE (2012): Global Fraud Study. Report to the Nations on Occupational Fraud and Abuse. 4 ff.

12 Die Kosten von Internetkriminalität in Deutschland wurden von McAfee und dem Center for Strategic and International Studies gemeinsam auf 1,6 Prozent des Bruttoinlandsprodukts geschätzt, also auf etwa 46 Milliarden Euro, McAfee (2014): Net Losses: Estimating the Global Cost of Cybercrime. Center for Strategic and International Studies, 5 f. Von Symantec wurden die Kosten durch Cybercrime in Deutschland im Jahr 2013 auf umgerechnet etwa 3,5 Milliarden Euro insgesamt sowie etwa 240 Euro pro Geschädigten geschätzt, Symantec (2013): Norton Report 2013. www.symantec.com/content/en/us/about/presskits/b-norton-report-2013.de_de.pdf, Zugriff am 23.02.2015.

13 Kosten für Bürger des Vereinigten Königreichs belaufen sich im Bereich Identitätsdiebstahl laut Detica-Report auf umgerechnet 2,3 Milliarden Euro, bei Online-Betrug auf 1,9 Milliarden Euro sowie bei sogenannten "Scareware" und falschen Antivirusprogrammen auf 41 Millionen Euro, siehe Detica (2011): The Cost of Cybercrime. A Detica Report in Partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office, 18, www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf, Zugriff am 19.02.2015.

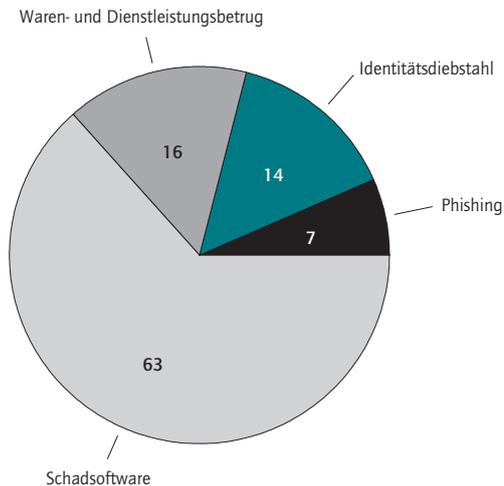
14 Die Angaben von 217 der insgesamt 12 094 Befragten finden in dieser Studie aufgrund fehlender Teilinformationen keine Berücksichtigung.

15 Siehe hierzu auch die Pressemitteilung zum „Bundeslagebild Cybercrime 2013“ von Bundeskriminalamt und BITKOM: „Nach einer repräsentativen BITKOM-Umfrage unter 1 000 Internetnutzern in Deutschland sind mit 55 Prozent mehr als die Hälfte in den vergangenen 12 Monaten Opfer von Internetkriminalität geworden. Das entspricht rund 29 Millionen Betroffenen.“ Dort werden auch nicht folgenschwere Infektionen mit Schadprogrammen sowie weitere Kategorien von Internetkriminalität eingerechnet. www.bka.de/DE/Presse/Pressemitteilungen/Presse2014/140827_BundeslagebildCybercrime.html?__nnn=true, Zugriff am 03.03.2015; ferner Frankfurter Allgemeine Zeitung, 28.08.2014, 15. Die schufa errechnete für 2013 auf Basis einer Umfrage einen Anteil der Opfer von Identitätsdiebstahl oder -missbrauch von 21 Prozent. www.schufa.de/de/private/presse/aktuellepressemittelungen/130913_jeder_fuenfte_deutsche_war_bereits_opfer_eines_identitaetsdiebstahls.jsp, Zugriff am 11.03.2014.

Abbildung 1

Bedeutung der einzelnen Kategorien von Internetkriminalität

Anteile an der Gesamtzahl der Fälle in Prozent



Quellen: Befragung im Rahmen des WISIND-Projekts; eigene Berechnungen.

© DIW Berlin 2015

Delikte mit Schadsoftware sind die mit Abstand dominierende Form von Internetkriminalität.

Internetkriminalität entfallen 63 Prozent auf Delikte mit Schadsoftware (Abbildung 1).¹⁶ Dabei sind solche Fälle bereits herausgerechnet, die aufgrund von automatisierten Abwehrmaßnahmen (zum Beispiel Antivirus-Software) nach Auskunft der Betroffenen zu keinem weiteren Schaden führten.

Auch unter Berücksichtigung der Bevölkerungsgröße und trotz der „grenzenlosen“ Natur von Internetkriminalität – bei dem der Erfolgsort meist fern des Tatbegehungsortes liegt – lassen sich deutliche Unterschiede zwischen den Bundesländern erkennen (Tabelle 1). Die in der Tabelle dargestellte stärkere Betroffenheit der alten gegenüber den neuen Bundesländern könnte zum einen durch unterschiedliche infrastrukturelle Möglichkeiten der Internetnutzung erklärt werden. Zum anderen haben der demografischer Wandel und die Landflucht in bestimmten Bundesländern zur Folge, dass anteilig weniger Internetnutzer dort leben. Auch dies könnte erklären, warum die Fallzahlen der Internetkriminalität hier pro Kopf niedriger sind. Ein bun-

16 Aufgrund des Mindestalters der Befragten von 16 Jahren könnte die Hochrechnung auf die Gesamtbevölkerung – der auch jüngere, das Internet nicht für Transaktionen nutzende Personen angehören – die Schadenshöhe etwas überschätzen.

Kasten

Bevölkerungsbefragung zu Internetkriminalität

Im Rahmen des WISIND-Projekts wurde von TNS Emnid eine repräsentative computergestützte Telefonbefragung zwischen Juli und September 2014 von 12 094 Personen durchgeführt. 20 Prozent der Befragten wurden per Mobilfunknummer angerufen, um einen systematischen Ausschluss von Personen ohne Festnetzanschluss zu vermeiden. Alle Befragten waren aus rechtlichen Gründen mindestens 16 Jahre alt. Pro Landkreis wurden mindestens 15 Telefonnummern zufällig ausgewählt, darüber hinaus waren die Landkreise proportional zu ihrer Bevölkerungsgröße vertreten. Innerhalb des erreichten Haushaltes wurde der Gesprächspartner nach einem Zufalls-Auswahlverfahren bestimmt. Den Gesprächspartnern wurden zum Bereich Internetkriminalität folgende Fragen gestellt:

Wortlaut der Fragen ...

... *bezogen auf die Zahl der Fälle (Viktimisierung)*

Phishing: „Wurde seit Anfang 2012 bis heute Ihr Kredit- oder Bankkonto durch jemanden unrechtmäßig belastet, der Ihre geheimen Passwörter über das Internet betrügerisch erlangt hat?“

Antwortkategorien: „Ja“; „Nein“; „Weiß nicht“; „Verweigert“

„Wie oft wurden Sie in den Jahren 2012 bis heute insgesamt Opfer von Online-Kontomissbrauch?“

Antwortkategorien: „Einmal“; „Zweimal“; „Dreimal“; „Mehr als dreimal, *bitte genaue Anzahl angeben*“; „Weiß nicht“; „Verweigert“

Identitätsdiebstahl: „Wenn Sie von heute bis Anfang 2012 zurückblicken, wurden Ihre persönlichen Daten in diesem Zeitraum missbraucht?“ (Antwortkategorien siehe Phishing)

„Wie viele Fälle von Identitätsdiebstahl haben Sie in den Jahren seit 2012 insgesamt erlitten?“ (Antwortkategorien siehe Phishing)

Waren- und Dienstleistungsbetrug via Internet: „Wenn Sie von heute bis Anfang 2012 zurückblicken, wurden Sie persönlich in diesem Zeitraum Opfer von Waren- und Dienstleistungsbetrug im Internet?“ (Antwortkategorien siehe Phishing)

„Wie viele Fälle von Waren- und Dienstleistungsbetrug im Internet haben Sie in den Jahren seit 2012 insgesamt erlitten?“ (Antwortkategorien siehe Phishing)

Schadsoftware: „Wenn Sie von heute bis Anfang 2012 zurückblicken, war mindestens eines Ihrer privaten Geräte, egal ob Computer, Smartphone oder Tablet, von Schadsoftware befallen?“ (Antwortkategorien siehe Phishing)

„Wie oft wurden Sie in den Jahren seit 2012 insgesamt Opfer von Schadsoftware?“ (Antwortkategorien siehe Phishing)

... *bezogen auf die Schadenssummen*

Phishing: „Können Sie angeben, wie hoch Ihr finanzieller Schaden, alles mit eingerechnet, in Folge des jüngsten Online-Kontomissbrauchs war?“

Antwortkategorien: „Betrag eingeben“; „Weiß nicht“; „Verweigert“

„Und können Sie sich vielleicht daran erinnern, wenn Sie die folgenden Geldstufen im Blick haben? Waren das...“

Antwortkategorien: „Bis zu 100€“; „Bis zu 500€“; „Bis zu 1 000€“; „Bis zu 3 000€“; „Bis zu 10 000€“; „Mehr als 10 000€“; „Weiß nicht“; „Verweigert“

Identitätsdiebstahl: „Können Sie angeben, wie hoch Ihr finanzieller Schaden, alles mit eingerechnet, in Folge des jüngsten Identitätsdiebstahls war?“ (Antwortkategorien siehe Phishing)

„Und können Sie sich vielleicht daran erinnern, wenn Sie die folgenden Geldstufen im Blick haben? Waren das...“ (Antwortkategorien siehe Phishing)

Waren- und Dienstleistungsbetrug via Internet: „Können Sie angeben, wie hoch Ihr finanzieller Schaden, alles mit eingerechnet, in Folge des jüngsten Waren- oder Dienstleistungsbetruges war?“ (Antwortkategorien siehe Phishing)

„Und können Sie sich vielleicht daran erinnern, wenn Sie die folgenden Geldstufen im Blick haben? Waren das...“ (Antwortkategorien siehe Phishing)

Schadsoftware: „Welche der folgenden Antworten treffen auf Ihren Fall zu?“ *Mehrfachnennungen möglich:* „Die Schadsoftware konnte sofort unschädlich gemacht werden“; „Die Schadsoftware konnte erst nach längerer Reparatur unschädlich gemacht werden“; „Die Schadsoftware zerstörte das Gerät“; „Daten gingen dauerhaft verloren“; „Weiß nicht“; „Verweigert“

Tabelle 1

Fälle von Internetkriminalität pro Jahr
Je 100 000 Einwohner

	Internetkriminalität insgesamt	Phishing	Identitätsdiebstahl	Waren- und Dienstleistungsbetrug	Schadsoftware
Baden-Württemberg	20 517	1 436	3 004	3 440	12 637
Bayern	18 404	929	3 017	3 217	11 241
Berlin	22 186	1 908	4 135	3 181	12 962
Brandenburg	16 763	1 099	1 763	1 964	11 936
Bremen	16 842	812	1 582	2 030	12 418
Hamburg	19 737	1 554	3 730	3 419	11 034
Hessen	17 827	1 452	2 219	3 639	10 518
Mecklenburg-Vorpommern	16 373	836	2 035	1 512	11 990
Niedersachsen	18 222	1 198	2 563	3 979	10 481
Nordrhein-Westfalen	18 084	1 262	3 056	2 600	11 166
Rheinland-Pfalz	18 854	997	1 265	3 070	13 522
Saarland	23 156	1 578	2 594	3 844	15 141
Sachsen	14 601	786	2 497	2 211	9 107
Sachsen-Anhalt	14 225	798	3 079	2 392	7 956
Schleswig-Holstein	17 254	1 782	2 698	2 676	10 097
Thüringen	16 420	574	2 634	1 837	11 375

Quellen: Bug, M., Kroh, M., Meier, K., Rieckmann, J., van Um, E., Wald, N. (2015): WISIND-Datensätze: Kriminalitätsbefragung; Berechnungen des DIW Berlin.

© DIW Berlin 2015

Trotz der „grenzenlosen“ Natur von Cybercrime variieren die Fallzahlen zwischen den Bundesländern deutlich.

desweites Stadt-Land-Gefälle lässt sich aus den Zahlen dagegen nicht erkennen.

Internetkriminalität ist kostspielig für betroffene Bürger

Die Höhe des Schadens, die sich aus den Angaben der Befragten ergibt, variiert je nach Deliktform (Tabelle 2).¹⁷ Die Opfer werden am stärksten durch Phishing geschädigt, im Durchschnitt kostet es den Bürger 814 Euro, wenn er Opfer eines Phishing-Deliktens wird. Allerdings werden in diesem Bereich laut Angaben der Repräsentativbefragung auch die höchsten Kompensationszahlungen durch Versicherungen geleistet.

¹⁷ Die insgesamt entstandenen Schadenssummen wurden basierend auf der Angabe zum jüngsten Vorfall berechnet, da sich die Befragten an diesen vermutlich am genauesten erinnern konnten. Bei Fällen, in denen der Befragte keine Summe direkt nennen konnte oder wollte, jedoch eine Spanne angab, wurde die Mitte der Spanne als Wert angenommen (Formel: (Untergrenze + Obergrenze)/2). Bei Befall mit Schadsoftware wurden im Interesse einer konservativen Schadensschätzung 0 Euro für dauerhaften Datenverlust angesetzt, 50 Euro für eine längere Reparatur und 500 Euro für zerstörte Geräte. Fälle, bei denen die Schadsoftware sofort unschädlich gemacht werden konnte, werden nicht als Schadensfälle betrachtet. Die Studie unterliegt wie die meisten Bevölkerungsbefragungen Vorbehalten im Hinblick auf erinnerungs-basierte quantitative Auskünfte. Daher sollten die Ergebnisse als Größenordnungen, nicht aber als präzise Messwerte aufgefasst werden.

Tabelle 2

Schaden durch Internetkriminalität je Fall
In Euro

	Schaden ...	
	insgesamt	abzüglich Versicherungsleistung
Phishing	814	295
Identitätsdiebstahl	402	-
Waren- und Dienstleistungsbetrug	238	201
Schadsoftware	129	-

Quellen: Bug, M., Kroh, M., Meier, K., Rieckmann, J., van Um, E., Wald, N. (2015): WISIND-Datensätze: Kriminalitätsbefragung; Berechnungen des DIW Berlin.

© DIW Berlin 2015

Opfer werden am stärksten durch Phishing geschädigt, allerdings greifen hier auch anschließende Entschädigungen am stärksten.

Relative Schadenshöhen lassen sich auf Bundeslandebene darstellen. Dafür wurden auf Basis der durchschnittlichen Schadenshöhe für einen einzelnen Fall der jeweiligen Internetkriminalität-Kategorie sowie der auf Basis der Stichprobe hochgerechneten Fallzahl je 100 000 Einwohner im jeweiligen Bundesland errechnet (Tabelle 3). Über alle Kategorien von Internetkriminalität betrachtet scheint die Berliner Bevölkerung am

Tabelle 3

Schaden¹ durch Internetkriminalität nach Bundesländern

Euro je Einwohner und Jahr

	Internetkriminalität insgesamt	Phishing	Identitätsdiebstahl	Waren- und Dienstleistungsbetrug	Schadsoftware
Baden-Württemberg	48	12	12	8	16
Bayern	42	8	12	8	14
Berlin	56	16	17	8	17
Brandenburg	36	9	7	5	15
Bremen	34	7	6	5	16
Hamburg	50	13	15	8	14
Hessen	43	12	9	9	14
Mecklenburg-Vorpommern	34	7	8	4	15
Niedersachsen	43	10	10	9	13
Nordrhein-Westfalen	43	10	12	6	14
Rheinland-Pfalz	38	8	5	7	17
Saarland	52	13	10	9	19
Sachsen	33	6	10	5	12
Sachsen-Anhalt	35	6	12	6	10
Schleswig-Holstein	45	15	11	6	13
Thüringen	34	5	11	4	15

¹ Ohne Berücksichtigung von Entschädigungsleistungen durch Versicherungen.

Quellen: Bug, M., Kroh, M., Meier, K., Rieckmann, J., van Um, E., Wald, N. (2015): WISIND-Datensätze: Kriminalitätsbefragung; Berechnungen des DIW Berlin.

© DIW Berlin 2015

Berliner Bürger erleiden im Ländervergleich pro Kopf die höchsten Schäden.

stärksten betroffen. Bei Betrachtung einzelner Kategorien schlägt Schadsoftware im Saarland am heftigsten zu Buche – ausschlaggebend dafür ist die hohe Fallzahl.

Schätzung des direkten Gesamtschadens übertrifft die der Polizei um den Faktor 50

Durch die einfache Multiplikation des durchschnittlichen Schadens pro Fall mit der aus der Stichprobe errechneten Fallhäufigkeit pro Jahr lässt sich größenordnungsmäßig der volkswirtschaftliche Gesamtschaden durch Internetkriminalität in Deutschland abschätzen. Sekundäreffekte wie ein gesteigerter Umsatz des Elektronik-Einzelhandels, der Verzicht auf Transaktionen aus Sicherheitsgründen oder Auswirkungen auf die Versicherungswirtschaft finden hier keine Berücksichtigung. Auch unter Berücksichtigung der begrenzten Verlässlichkeit von Erinnerungsdaten sowie der tendenziell überschätzenden Verzerrung durch Hochrechnung auch auf nicht das Internet nutzende Bevölkerungsteile muss von erheblichen Schäden durch Internetkriminalität ausgegangen werden.

Treffen die Angaben größenordnungsmäßig zu, so könnten allein durch Delikte aus dem Bereich Schad-

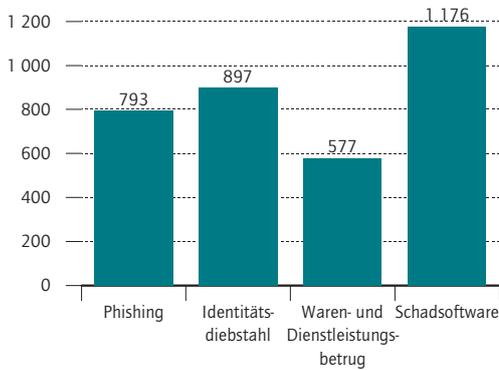
software bundesweit Privatleuten annähernd 1,2 Milliarden Euro an direkten jährlichen Schäden entstanden sein (Abbildung 2) – oder anders ausgedrückt, etwa 14,70 Euro pro Jahr für jeden Bundesbürger. Im Bereich Identitätsdiebstahl beträgt der Schaden pro Kopf rechnerisch etwa elf Euro, für Phishing fast zehn Euro sowie für Waren- und Dienstleistungsgut sieben Euro. Schadsoftware (mit erkannten Folgen) verursacht also den höchsten Schaden, Waren- und Dienstleistungsbetrug dagegen nur etwa die Hälfte. Auf die abgebildeten Internetkriminalität-Kategorien insgesamt entfallen – ohne Berücksichtigung von Entschädigungsleistungen durch Versicherungen – nach unseren Berechnungen etwa 3,4 Milliarden Euro, anders ausgedrückt 0,1 Prozent des deutschen Bruttoinlandsproduktes.

Am nächsten an den hier geschätzten Werten liegen unter den angeführten Quellen die der Studie von Symantec (vgl. Fußnote 11). Die Schätzung des Bundeskriminalamtes zu beispielsweise Schäden durch Phishing ist offenbar deutlich zu konservativ, unsere Berechnungen ergeben einen um den Faktor 50 höheren Schaden – und liegen damit nicht an der Spitze. Die Zahlen des Detica-Reports (vgl. Fußnote 12) zu den Gesamtschäden für Großbritannien liegen 2,5 Mal (Identitätsdiebstahl) bis 3,3 Mal (Waren- und Dienstleistungsbetrug im Inter-

Abbildung 2

Volkswirtschaftlicher Schaden durch Internetkriminalität gegen Privatpersonen

In Millionen Euro ohne Sekundäreffekte



Quellen: Bug, M., Kroh, M., Meier, K., Rieckmann, J., van Um, E., Wald, N. (2015): WISIND-Datensätze: Kriminalitätsbefragung; Berechnungen des DIW Berlin.

© DIW Berlin 2015

Schadsoftware verursacht den höchsten Schaden, Waren- und Dienstleistungsbetrug nur knapp die Hälfte davon.

net) höher als die Schätzung in diesem Beitrag. Die gemeinsame Schätzung des Center for Strategic and International Studies und des Sicherheitstechnologie-Anbie-

Johannes Rieckmann ist Wissenschaftlicher Mitarbeiter in der Abteilung Entwicklung und Sicherheit am DIW Berlin | jriekmann@diw.de

ters McAfee für Deutschland erscheint jedoch um ein zweistelliges Vielfaches zu hoch.¹⁸

Fazit

Die Auswertung einer breit angelegten Befragung gestattet erstmals für Deutschland Aussagen zur Größenordnung der Betroffenheit von Privatpersonen durch Internetkriminalität sowie zu den dadurch entstandenen finanziellen Schäden. Ein sehr großer Teil der Delikte wird von der polizeilichen Kriminalitätsstatistik nicht erfasst. Die Dunkelfeld-Ausleuchtung in Verbindung mit den Selbstauskünften der Befragten führt zu weit realistischeren Schadensschätzungen. Die jährlich entstehenden Schäden durch Internetkriminalität sind nicht nur für das Gewerbe, sondern auch für Privatpersonen erheblich. In vier besonders bedeutenden Kategorien der Internetkriminalität – Phishing, Identitätsbetrug, Waren- und Dienstleistungsbetrug sowie Angriffe mit Schadsoftware – belaufen sie sich auf insgesamt 3,4 Milliarden Euro pro Jahr, das entspricht 0,1 Prozent des deutschen Bruttoinlandsprodukts.

¹⁸ Zur Spannweite bisheriger Schätzungen siehe auch Hyman, P. (2013): Cybercrime: It's serious, but exactly how serious? Communications of the ACM, Vol 56 (3), 18 f., www.yildiz.edu.tr/~aktas/courses/CE-0112822/15-04-2-1.pdf, Zugriff am 26.02.2015; McAfee (2013): The Economic Impact of Cyber Crime and Cyber Espionage. Center for Strategic and International Studies, 10-17, csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf, Zugriff am 11.03.2015.

Martina Kraus ist studentische Hilfskraft in der Abteilung Entwicklung und Sicherheit am DIW Berlin | mkraus@diw.de

CYBERCRIME: DAMAGES RUN INTO BILLIONS

Abstract: Cybercrime can lead to considerable costs for those affected. Previous attempts to quantify the damage have focused mainly on businesses. Official information on damages incurred by individuals is based primarily on cases reported to the police, but these figures in no way accurately reflect the actual number of cybercrimes. This study, which is

based on a broadly conceived survey, evaluates the financial harm to individuals. It covers four key areas of cybercrime—phishing, identity theft, consumer fraud, and malicious software. The damage in these areas together amounts to approximately 3.4 billion euros per year, equivalent to 0.1 percent of Germany's gross domestic product (GDP).

JEL: H79, K42, L86, R12, Z18

Keywords: crime, crime statistics, cybercrime, darkfield, fraud, identity theft, indicator, inner security, malware, perception, phishing, police statistics, security



DIW Berlin – Deutsches Institut
für Wirtschaftsforschung e.V.
Mohrenstraße 58, 10117 Berlin
T +49 30 897 89 -0
F +49 30 897 89 -200
82. Jahrgang

Herausgeber

Prof. Dr. Pio Baake
Prof. Dr. Tomaso Duso
Dr. Ferdinand Fichtner
Prof. Marcel Fratzscher, Ph.D.
Prof. Dr. Peter Haan
Prof. Dr. Claudia Kemfert
Dr. Kati Krähnert
Prof. Karsten Neuhoff, Ph.D.
Prof. Dr. Jürgen Schupp
Prof. Dr. C. Katharina Spieß
Prof. Dr. Gert G. Wagner

Chefredaktion

Sabine Fiedler
Dr. Kurt Geppert

Redaktion

Renate Bogdanovic
Andreas Harasser
Sebastian Kollmann
Dr. Claudia Lambert
Marie Kristin Marten
Dr. Wolf-Peter Schill

Lektorat

Alexander Eickelpasch
Dr. Anika Rasner
Dr. David Richter
Dr. Dirk Ulbricht
Dr. Lilo Wagne

Pressestelle

Renate Bogdanovic
Tel. +49-30-89789-249
presse@diw.de

Vertrieb

DIW Berlin Leserservice
Postfach 74
77649 Offenburg
leserservice@diw.de
Tel. (01806) 14 00 50 25
20 Cent pro Anruf
ISSN 0012-1304

Gestaltung

Edenspiekermann

Satz

eScriptum GmbH & Co KG, Berlin

Druck

USE gGmbH, Berlin

Nachdruck und sonstige Verbreitung –
auch auszugsweise – nur mit Quellen-
angabe und unter Zusendung eines
Belegexemplars an die Serviceabteilung
Kommunikation des DIW Berlin
(kundenservice@diw.de) zulässig.

Gedruckt auf 100 % Recyclingpapier.