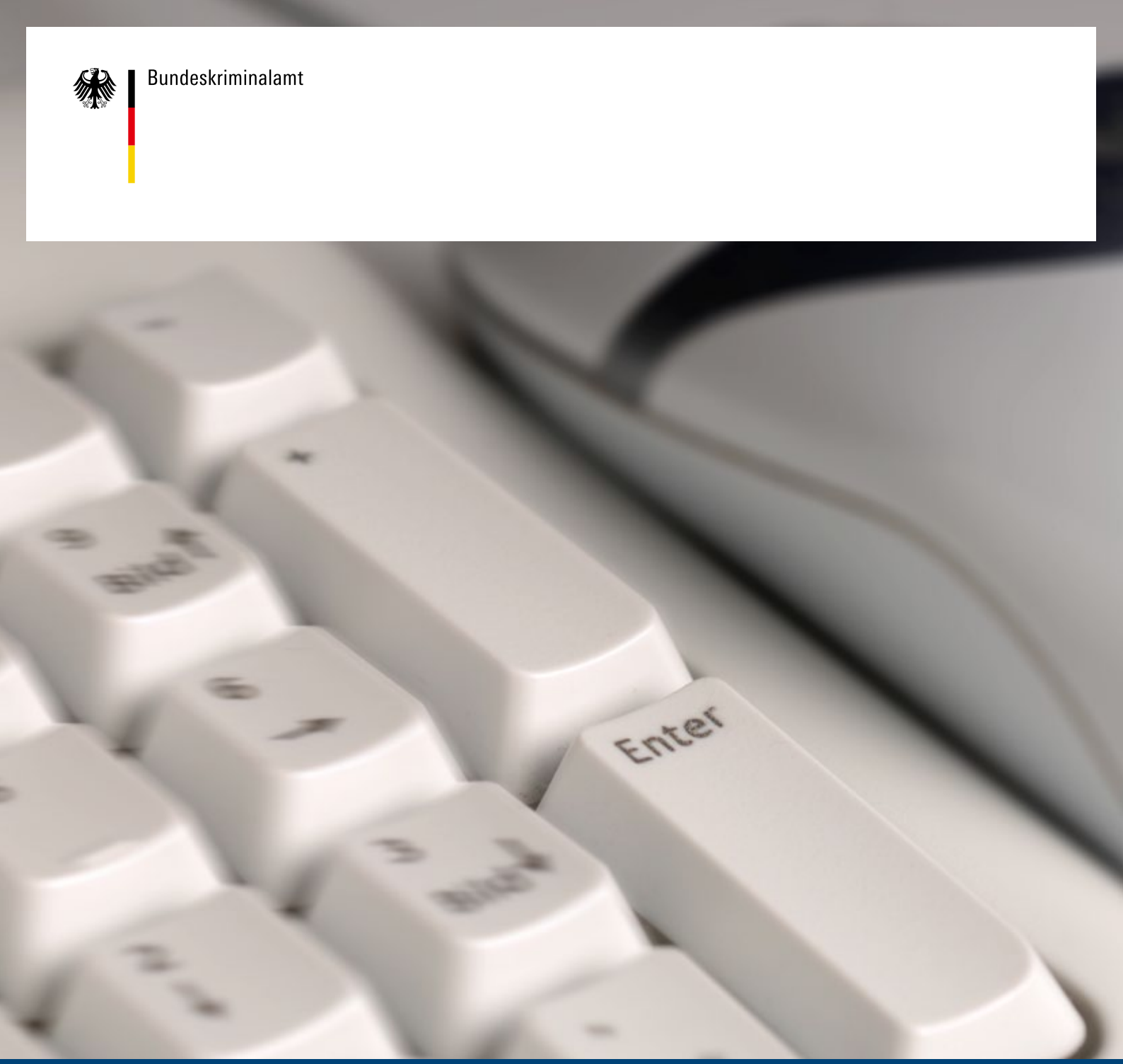
Bundeskriminalamt



Cybercrime

Bundeslagebild 2012

INHALT

1. VORBEMERKUNG

Das Lagebild informiert zu den Entwicklungen im Berichtszeitraum und beschreibt das Gefahren- und Schadenspotenzial von Cybercrime und deren Bedeutung für die Kriminalitätslage in Deutschland. Cybercrime umfasst die Straftaten, die sich gegen das Internet, weitere Datennetze, informationstechnische Systeme oder deren Daten richten. Cybercrime umfasst auch solche Straftaten, die mittels dieser Informationstechnik begangen werden.

Grundlage für den statistischen Teil des Lagebildes sind die Daten aus der Polizeilichen Kriminalstatistik (PKS). Basis für die phänomenologischen Aussagen des Lagebildes sind sowohl Erkenntnisse aus dem kriminalpolizeilichen Nachrichtenaustausch zu Sachverhalten der Kriminalität im Zusammenhang mit Cybercrime als auch externe Quellen.

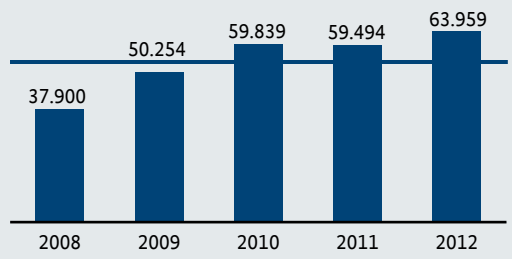
2. DARSTELLUNG UND BEWERTUNG DER KRIMINALITÄTSLAGE

2.1 POLIZEILICHE KRIMINALSTATISTIK

Anstieg der Fälle von Cybercrime

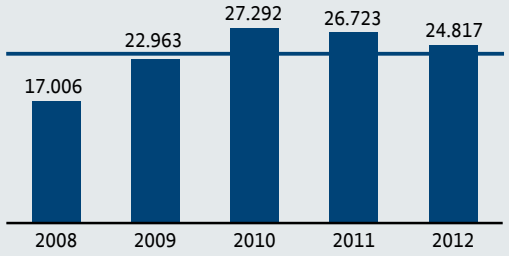
Die Zahl der in der PKS erfassten Fälle von Cybercrime, also aller Straftaten, die unter Ausnutzung moderner Informations- und Kommunikationstechnik oder gegen diese begangen wurden, stieg im Jahr 2012 auf 63.959 Fälle. Dies entspricht einer Steigerung von 8 % gegenüber dem Vorjahr.

Cybercrime im engeren Sinne 2008-2012 (PKS)[01]

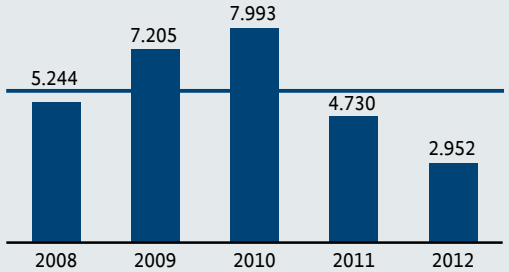


Eine Betrachtung der einzelnen Deliktsbereiche ergibt im Fünf-Jahres-Vergleich folgendes Bild:

Computerbetrug 2008-2012 (PKS)

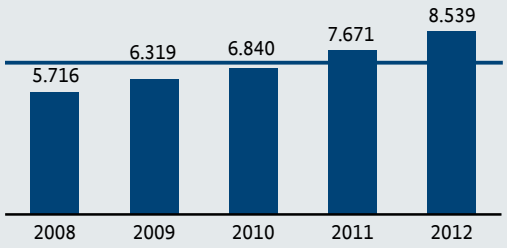


Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten 2008-2012 (PKS)



01 Umfasst die Delikte: Computerbetrug (PKS 517500), Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten (PKS 517900), Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung (PKS 543000), Datenveränderung/ Computersabotage (PKS 674200) sowie Ausspähen, Abfangen von Daten einschl. Vorbereitungshandlungen (PKS 67800).

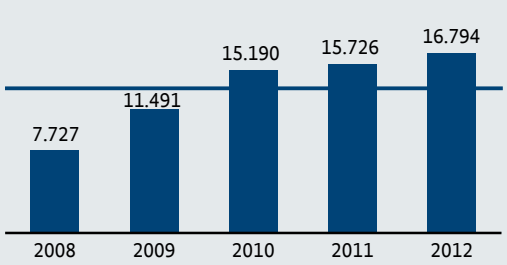
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung 2008-2012 (PKS)



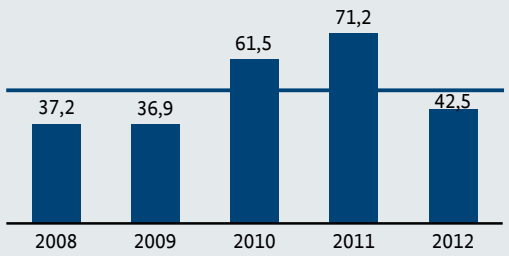
Rückgang bei Schäden durch Cybercrime

Bei den registrierten Schäden ist ein Rückgang um rund 40 % auf rund 42,5 Mio. Euro zu verzeichnen (2011: 71,2 Mio. Euro). Davon entfallen rund 33,6 Mio. Euro auf den Bereich Computerbetrug und rund 2,7 Mio. Euro auf den Betrug mit Zugangsdaten zu Kommunikationsdiensten[02]. Die Tatsache, dass zu lediglich zwei Deliktsbereichen eine statistische Schadenserfassung erfolgt, lässt zwar keine belastbaren Aussagen zum tatsächlichen monetären Schaden im Bereich Cybercrime zu, reicht aber nach hiesiger Einschätzung aus, um mittel- und langfristig zumindest Entwicklungstendenzen darzustellen.

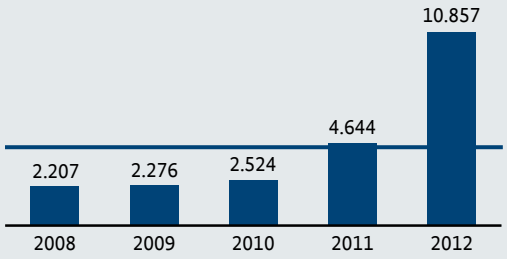
Ausspähen/Abfangen von Daten 2008-2012 (PKS)



Schäden 2008 - 2012 (in Mio. Euro) (PKS)



Datenveränderung, Computersabotage 2008-2012 (PKS)



Eine Einschätzung des Phänomens Cybercrime allein auf Basis statistischer Zahlen ist nicht möglich. Einzelne bzw. besonders relevante Phänomene, wie z. B. Phishing im Bereich Onlinebanking, Epressungshandlungen im Zusammenhang mit gezielten DDoS-Attacken[03] oder auch die vielfältigen anderen Erscheinungsformen der digitalen Erpressung (z. B. die sogenannte „Ransomware"), werden in der PKS nicht unter dem Begriff Cybercrime, sondern vielmehr unter den PKS-Schlüsseln der einzelnen Tathandlungen erfasst.

Die mit Abstand größte Straftatengruppe ist der Computerbetrug mit einem Anteil von rund 39 % aller Fälle. Deutliche Veränderungen zeigen sich in den Deliktsbereichen Datenveränderung/Computersabotage (+ 134 %), Datenfälschung, Täuschung im Rechtsverkehr bei Datenverarbeitung (+ 11 %) sowie beim Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten (- 37,5 %).

02 Eine Erfassung der Schadenssumme erfolgt lediglich bei den Delikten Computerbetrug (PKS 517500) und Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten (PKS 517900).

03 Bei DDoS (Distributed Denial of Service)-Angriffen rufen alle in einem Botnetz zusammengeschlossenen Zombie-PC auf Befehl des Botmasters innerhalb kürzester Abstände immer wieder z. B. eine nicht existente Seite auf den Webservern der angegriffenen Firma auf. Diese Seitenaufrufe werden so lange fortgesetzt, bis die Webserver unter der Last der Anfragen zusammenbrechen und damit ihren Service verweigern (Denial of Service), so dass die jeweilige Firmenpräsenz damit nicht mehr über das Internet erreichbar ist.

Großes Dunkelfeld

Hinzu kommt das vermutete große Dunkelfeld, insbesondere bei den Deliktsfeldern Computersabotage und Datenveränderung, da

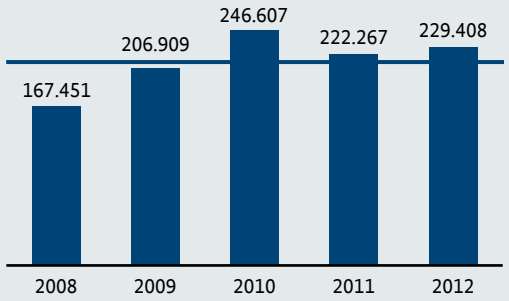
- eine große Anzahl der Straftaten aufgrund immer weiter verbreiteter technischer Sicherungseinrichtungen über das Versuchsstadium nicht hinauskommt und von den Geschädigten nicht angezeigt wird, zumal meist kein finanzieller Schaden entsteht.
- Straftaten durch den Geschädigten nicht erkannt werden (die Infektion des Computers bleibt unentdeckt) oder
- der Geschädigte (häufig ein Unternehmen) die erkannte Straftat nicht anzeigt, um beispielsweise im Kundenkreis die Reputation als „sicherer und zuverlässiger Partner“ nicht zu verlieren.

Solche Straftaten gelangen oftmals nicht zur Anzeige und somit nicht zur Kenntnis der Strafverfolgungsbehörden. Infolgedessen wird nicht nur eine erfolgreichere Bekämpfung von Cybercrime verhindert. Diese Informationen dienen den Strafverfolgungsbehörden auch als Grundlage zur Optimierung bestehender und Entwicklung neuer Präventions- und Bekämpfungsstrategien und tragen somit letztlich zu einem erhöhten Schutz aller Nutzer von informationstechnischen Systemen bei.
Unabhängig von der Entwicklung der reinen Fall- bzw. Schadenszahlen, die aufgrund des vermuteten Dunkelfeldes ohnehin nur eine sehr begrenzte Aussagekraft besitzen, haben die Intensität der kriminellen Aktivitäten im Bereich Cybercrime und das für jeden Internetnutzer bestehende Gefährdungspotenzial weiter zugenommen. Diese Entwicklung lässt sich nicht zuletzt an der gestiegenen Professionalität der eingesetzten Schadsoftware ablesen. Auch sich ständig ändernde Modi Operandi zeigen, wie flexibel, schnell und professionell die Täterseite auf neue technische Entwicklungen reagiert und ihr Verhalten entsprechend anpasst.
Erfolgte noch vor wenigen Jahren die Verbreitung von Malware[04] überwiegend in Form von Emailanhängen, wodurch eine tatsächliche „Infektion“ in aller Regel nur mittels einer Aktivität seitens des Opfers möglich war, so finden heute solche Angriffe z. B. in Form von Drive-By-Infections[05] ohne eigentliche „Fehl-“Aktivität des Opfers statt. Eine weitere, sich zunehmend verbreitende Variante ist die Verteilung der Malware über soziale Netzwerke, in denen das Opfer dem Infektor („seinem Freund“) vertraut, angebotene Dateien/Programme in gutem Glauben akzeptiert und dadurch sein System infiziert. Auch Instant-Messaging-Dienste (wie z. B. Skype oder der Facebook-Chat) werden mittlerweile verstärkt für die Auslieferung von Schadsoftware verwendet.
Zusätzlich dazu hat sich im Bereich der sog. Underground Economy[06] auch in Deutschland eine breite Szene etabliert, die sich zuvor überwiegend in englisch- oder russischsprachigen Foren und Plattformen betätigte. Die in den vergangenen Jahren gewachsene Forenlandschaft hat sich jedoch in den letzen ein bis zwei Jahren merklich verkleinert, was zum einen auf die gerade in diesem Bereich erfolgreichen Ermittlungsmaßnahmen der Strafverfolgungsbehörden, zum anderen aber auch auf ein deutlich höheres Sicherheitsbedürfnis der Straftäter und ihr Wissen um Aktivitäten der Strafverfolgungsbehörden zurückzuführen ist. Gerade im russischsprachigen Teil der Forenlandschaft ist eine deutliche Verlagerung auf andere Kommunikationskanäle festzustellen.

Internet als Tatmittel

Zur Abrundung des Gesamtbildes muss über die Betrachtungen der reinen Fallzahlen von Cybercrime hinaus auch ein Blick auf das Internet als Tatmittel geworfen werden.

Tatmittel Internet 2008-2012 (PKS)



04 Computerschadprogramm (Begriff aus dem Englischen; „malicious“ (bösartig) und „Software“).

05 Bezeichnet das unerwünschte Herunterladen von Schadsoftware allein durch das Anschauen einer dafür präparierten Webseite (engl. Drive-by: im Vorbeifahren).

06 Globaler, virtueller Marktplatz, über den kriminelle Anbieter und Käufer ihre Geschäfte rund um die digitale Welt tätigen, wie z. B. der Verkauf gestohlener digitaler Identitäten oder auch kompletter krimineller Infrastrukturen.

2.2 AKTUELLE PHÄNOMENE

Diebstahl digitaler Identitäten

Die digitale Identität ist die Summe aller Möglichkeiten und Rechte des einzelnen Nutzers sowie seiner Aktivitäten innerhalb der Gesamtstruktur des Internets. Konkret handelt es sich um alle Arten von Nutzer-Accounts, also zum Beispiel Zugangsdaten in den Bereichen

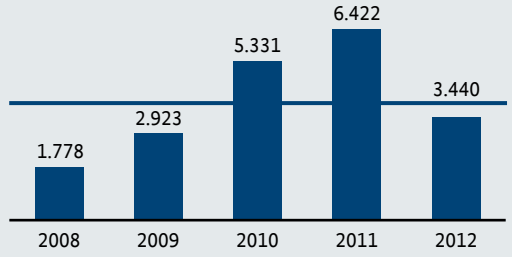
- Kommunikation (Email- und Messengerdienste),
- E-Commerce (Onlinebanking, Onlinebrokerage, internetgestützte Vertriebsportale aller Art),
- berufsspezifische Informationen (z. B. Nutzung eines Homeoffice für den Zugriff auf firmeninterne technische Ressourcen),
- E-Government (z. B. elektronische Steuererklärung) sowie
- Cloud-Computing.

Darüber hinaus sind auch alle anderen zahlungsrelevanten Informationen (insbesondere Kreditkartendaten einschließlich der Zahlungsadressen sowie weiterer Informationen) ebenfalls Bestandteil der digitalen Identität.
Die Täter nutzen heute überwiegend „trojanische Pferde“, um Eingaben des Besitzers bzw. Anmeldedaten und Transaktionen zu erlangen, und gehen dabei häufig arbeitsteilig und unter Nutzung hochprofessioneller Strukturen vor. Anschließend werden die Daten von weiteren Tätern kriminell eingesetzt.
Zudem treten Tätergruppierungen in Erscheinung, die bisher vorwiegend in anderen Phänomenbereichen (wie beispielsweise beim Betrug) aktiv waren, und mangels technischer Expertise nach wie vor traditionelle Modi Operandi (z. B. per Email übermittelte Links zu Phishing-Seiten) verwenden.

Rückläufige Fallentwicklung beim Phishing

Die bekannteste Variante des digitalen Identitätsdiebstahls ist das sog. „Phishing im Zusammenhang mit Onlinebanking“. Für das Jahr 2012 wurden dem Bundeskriminalamt 3.440 Sachverhalte im Phänomenbereich Phishing gemeldet. Im Vergleich zum Jahr 2011 (6.422) bedeutet dies einen Rückgang der Fallzahlen um rund 46 %.

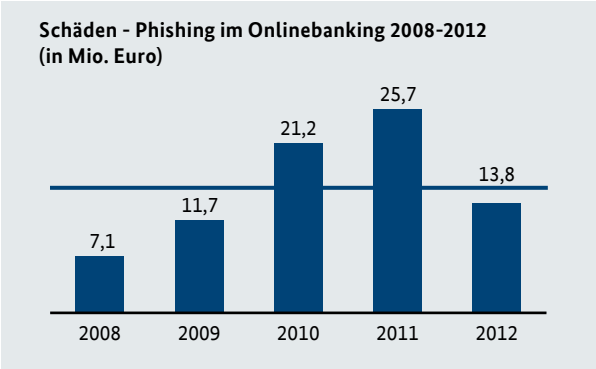
Fälle - Phishing im Onlinebanking 2008—2012



Nach dem seit 2008 festgestellten Trend steigender Fallzahlen in diesem Bereich erfolgt erstmals ein Rückgang der Fälle.
Dies ist zurückzuführen auf

- Sensibilisierung der Anwender,
- verstärkte Schutzmaßnahmen,
- effektives IT-Management.

Der Rückgang ist vor allem auch auf die verstärkte Anwendung von sog. „SMS-TAN“ als Sicherungsmethode im Rahmen des Onlinebanking-Marktes zurückzuführen. Hier reicht die Infektion des Rechners nicht mehr aus, stattdessen muss für den erfolgreichen Angriff nun auch der weitere Kommunikationskanal zum Kunden durch die Täterseite kontrolliert werden, indem das durch den jeweiligen Bankkunden genutzte Mobilfunktelefon mit einer passenden Schadsoftware (die bereits für die meisten Betriebssysteme existiert) infiziert wird.
Phishing bildet im Hinblick auf das vorhandene Schadenspotenzial und die Lukrativität für die Täterseite jedoch weiterhin einen Schwerpunkt im Bereich Cybercrime. So betrug die durchschnittliche Schadenssumme im Bereich „Phishing im Zusammenhang mit Onlinebanking“ im Jahr 2012 rund 4.000 Euro pro Fall. Auf dieser Berechnungsgrundlage ergeben sich unter Berücksichtigung der dem Bundeskriminalamt in den letzen vier Jahren gemeldeten Fallzahlen folgende ungefähre Schäden:



Hinsichtlich der im Bereich des Phishing im Onlinebanking täterseitig eingesetzten Schadsoftware gibt es keine grundlegend neuen Erkenntnisse. Derzeit befindet sich eine neue Schadsoftware für Android-basierte Endgeräte im Umlauf, die das mobile TAN-Verfahren im Onlinebanking umgehen soll. Die Besonderheit der Schadsoftware besteht insbesondere darin, dass zuvor keine Infektion eines Computers notwendig ist und dass eine Kontrolle der Schadsoftware auf dem Endgerät über das Internet (und nicht SMS-basiert) erfolgt. Die nunmehr festgestellte Schadsoftware ist nach hiesigem Kenntnisstand die erste für den deutschen Markt, die das direkte Abgreifen der Onlinebanking-Zugangsdaten beinhaltet. Weiterhin sind mehrere „Familien" von Schadsoftware in Form von Trojanern im Umlauf, die speziell auf den deutschen Bankenmarkt ausgerichtet sind und über das technische Potenzial verfügen, sowohl das iTAN- als auch das mTAN-Verfahren[07] mittels sog. Echtzeitmanipulation (Man-In-The-Middle / Man-in-the-Browser-Attacken[08]) erfolgreich anzugreifen.

Zunahme digitaler Erpressungen

Jeder Teilnehmer der digitalen Welt (Privatperson oder Unternehmen) kann Opfer einer solchen Erpressung werden. Selbst technische Laien, die entsprechendes Equipment oder auch die gesamte „Dienstleistung" in einschlägigen Foren der Underground Economy erwerben können, sind in der Lage, eine solche Erpressung durchzuführen. Nach Einschätzung des BKA hat sich diese Art von Erpressung weiter ausgebreitet, insbesondere in der Ausprägung von Forderungen nach „digitalem Lösegeld".

Eine bekannte Variante der derzeit im Internet kursierenden Ausprägungen von Ransomware ist der sogenannte angebliche „BKA-Trojaner". Hier wird dem Nutzer des mit der Schadsoftware infizierten Computers mittels einer eingeblendeten Meldung (mit Kopf Bundeskriminalamt?) suggeriert, dass der Computer im Zusammenhang mit verschiedenen strafbaren Handlungen in Erscheinung getreten und daher gesperrt worden sei.

Die Meldung informiert den Geschädigten weiterhin über die Möglichkeit einer Entsperrung des Computers nach Zahlung von 100 Euro. Dabei wird dem Geschädigten in der Regel die Möglichkeit der Bezahlung über digitale Zahlungsdienstleister angeboten, wodurch ein anonymer Geldtransfer vom Opfer zum Täter erfolgt. Mittlerweile sind weltweit mindestens 25 Staaten von diesem Phänomen betroffen. Angepasste Versionen der Ransomware sind zwischenzeitlich auch in Nord- und Südamerika (USA, Kanada, Mexico, Brasilien, Peru, Kolumbien, Argentinien) im Umlauf. Dieser Umstand resultiert u. a. aus der Möglichkeit, den Quellcode der Schadsoftware (seit Ende 2011) in entsprechenden Foren der Underground Economy zu kaufen.

Mobile Endgeräte – Smartphones als Angriffsziel

Mobile Endgeräte wie Smartphones stellen weiterhin ein interessantes Zielfeld für die Täter dar, da sich die Nutzer der Gefahr mobiler Betriebssysteme unzureichend bewusst sind.[09] Die Einsatzgebiete von Smartphones im täglichen Gebrauch werden zunehmend vielfältiger, z. B. im Bereich Onlinebanking zur Autorisierung von Transaktionen oder dem unmittelbaren Zugriff auf E-Mailkonten und Konten sozialer Netzwerke über entsprechende Apps.[10] Zunehmend werden immer mehr geschäftliche Daten unterwegs genutzt und über Mobilfunkverbindungen übertragen und ausgetauscht.

07 Mobile Transaktionsnummer – Anders als beim iTAN-Verfahren wird für jede Online-Überweisung eine eigene Transaktionsnummer generiert und per SMS an den Kunden übermittelt.

08 Bei einer „Man-In-The-Middle-Attacke" steht der Angreifer entweder physikalisch oder logisch zwischen den beiden Kommunikationspartnern und hat mit seinem System die Kontrolle über den Datenverkehr zwischen den Kommunikationspartnern. Dabei kann er die Informationen einsehen und manipulieren. Bei „Man-In-The-Browser-Attacken" manipuliert die auf dem Rechner mittels eines Trojaners installierte Malware die Kommunikation innerhalb des Webbrowsers, wodurch andere Informationen weitergegeben werden, als der Nutzer eingibt.

09 Im Jahr 2012 wurden in Deutschland 18 Millionen Smartphones verkauft (Quelle: GfK).

10 App (englisch) – application. Apps (in Zusammenhang mit Smartphones) sind Anwendungen, die über die Nutzung der Datenverbindung verschiedene Funktionen und Services erfüllen.

3. GESAMTBEWERTUNG

Die Bedrohungen durch Cybercrime im Rahmen von veränderten Erscheinungsformen der Kriminalität sind vielfältig. Das Internet bietet weltweit Tatgelegenheiten mit unzähligen potenziellen Opfern und Angriffspunkten. Daher ist das Gefährdungs- und Schadenspotenzial des Phänomens Cybercrime unverändert hoch. Neben den Zugangsdaten im Bereich des Onlinebanking werden alle Formen und Arten der digitalen Identität ausgespäht und für kriminelle Zwecke eingesetzt. Das Phänomen digitaler Erpressungen mittels sog. „Ransomware“ hat sich zu einem Massenphänomen im Bereich Cybercrime entwickelt. Daneben spielen, wenn auch in wesentlich geringerem Umfang, Straftaten im Rahmen des sog. „Hacktivismus“ eine Rolle.
Die bereits in den Vorjahren festgestellte Veränderung der erkannten Täterstrukturen hat sich im Berichtsjahr fortgesetzt. Es agieren nicht mehr nur hochspezialisierte Einzeltäter mit umfassenden IT-Kenntnissen, sondern vermehrt auch Kriminelle ohne spezifische Fachkenntnisse, die für die Begehung der Straftaten arbeitsteilig zusammenwirken. Die Täter begehen heute nicht mehr nur die Straftaten im eigentlichen Sinne, sondern bieten vielmehr die zur Begehung von Straftaten erforderliche Schadsoftware oder gar komplette kriminelle Infrastrukturen in der Underground Economy global zum Kauf oder zur Miete an. Diese Werkzeuge sind aufgrund ihrer einfachen Handhabung auch für Täter ohne fundierte IT-Spezialkenntnisse nutzbar. Insoweit ist das Profil der im Bereich Cybercrime agierenden Straftäter heterogen bei gleichzeitig hohem Innovationspotenzial. Dabei bereiten die Internationalität des Phänomens und die Anonymisierungsmöglichkeiten des Internets für die Cyber-Angreifer den Strafverfolgungsbehörden häufig Probleme, den Angreifer oder dessen Auftraggeber zu ermitteln. Erschwerend kommt hinzu, dass es in Deutschland hinsichtlich der Speicherung von Telekommunikationsverbindungsdaten weiterhin an sog. „Mindestspeicherungsfristen“ fehlt.
Die von den verschiedenen Facetten des Phänomens Cybercrime ausgehenden Gefahren sind in ihrem Ausmaß und in ihren Ausprägungen weiterhin bedeutsam. Nach Einschätzung des Bundeskriminalamts wird der Bereich Cybercrime auch in den kommenden Jahren ein wachsendes Phänomen darstellen, dessen Bekämpfung die Sicherheitsbehörden sowohl präventiv als auch repressiv im Sinne eines ganzheitlichen Ansatzes fortsetzen müssen.

IMPRESSUM

Herausgeber
Bundeskriminalamt
SO 51
65173 Wiesbaden

Stand
2012

Druck
BKA

Bildnachweis
Fotos: Polizeiliche Quellen

www.bka.de