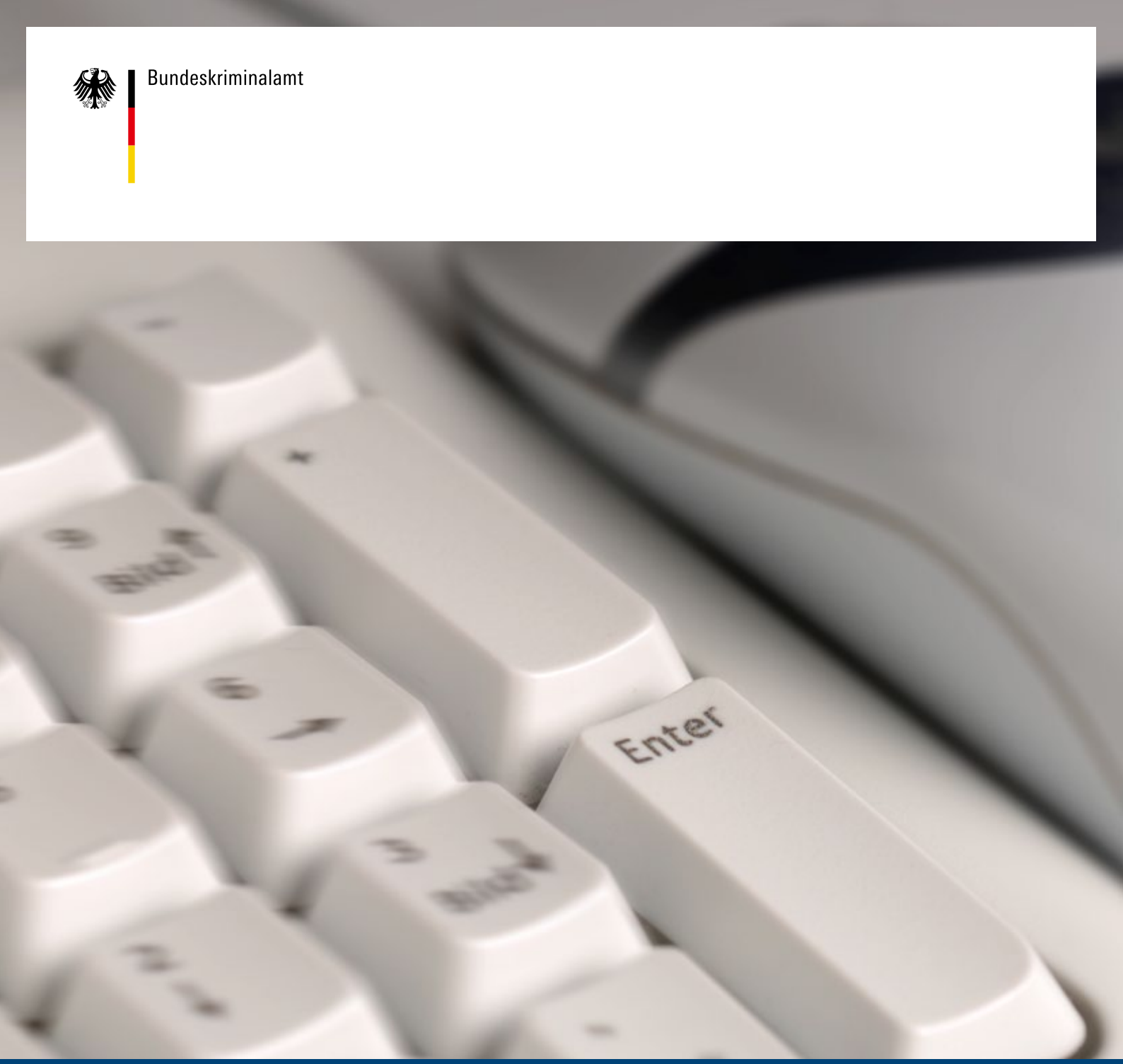
Bundeskriminalamt



Cybercrime

Bundeslagebild 2013

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, Datennetze, informationstechnische Systeme oder deren Daten richten,
- 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.

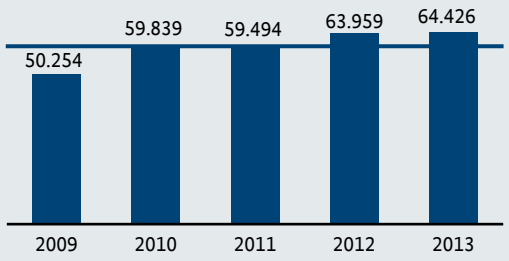
2 DARSTELLUNG UND BEWERTUNG DER KRIMINALITÄTSLAGE

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 2013 auf 64.426 Fälle. Dies entspricht einer Steigerung von rund 1 % gegenüber dem Vorjahr.

Cybercrime im engeren Sinne 2009-2013 (PKS)[01]

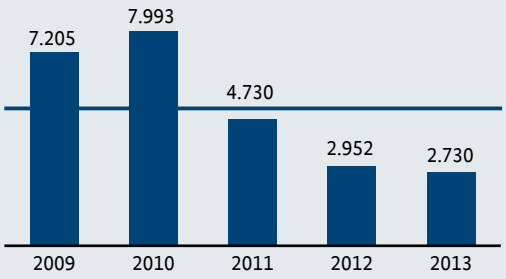


Eine Betrachtung der einzelnen Deliktsbereiche ergibt im Fünf-Jahres-Vergleich folgendes Bild:

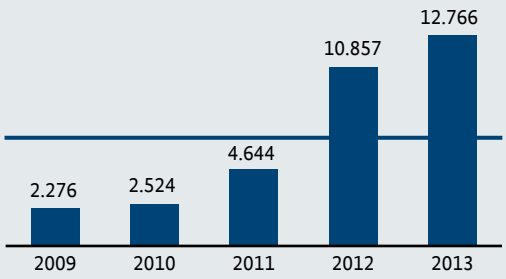
Computerbetrug 2009-2013 (PKS)

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).

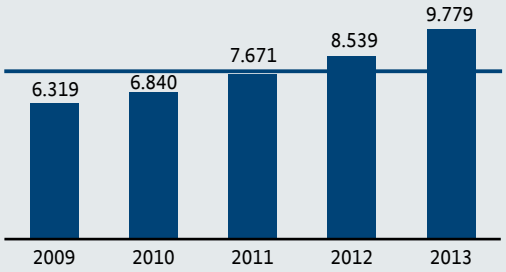
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten 2009-2013 (PKS)



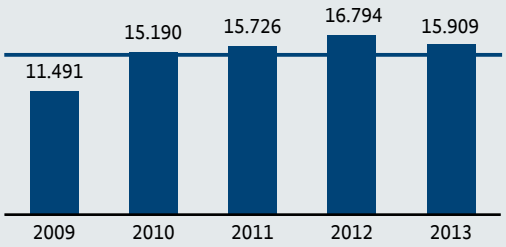
Datenveränderung, Computersabotage 2009-2013 (PKS)



Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung 2009-2013 (PKS)



Ausspähen/Abfangen von Daten 2009-2013 (PKS)



In den einzelnen Deliktsbereichen zeigt sich eine durchaus heterogene Entwicklung. Während in den Bereichen Computerbetrug, Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten und Ausspähen/Abfangen von Daten Rückgänge im mittleren einstelligen Bereich zu verzeichnen sind (zwischen 5 und 8 %), ergeben sich bei den Delikten Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung (rund 15 %) und Datenveränderung, Computersabotage (rund 18 %) Steigerungsraten im zweistelligen Bereich.
Einzelne bzw. besonders relevante Phänomene, wie z. B. Phishing im Bereich Onlinebanking, Erpressungshandlungen im Zusammenhang mit gezielten DDoS-Attacken[02] oder auch die vielfältigen anderen Erscheinungsformen der digitalen Erpressung (z.B. die sogenannte „Ransomware“[03], in der Öffentlichkeit vor allem bekannt als „BKA-Trojaner“ oder „GVU-Trojaner“), werden in der PKS nicht unter dem Begriff Cybercrime, sondern vielmehr unter den PKS-Schlüsseln der einzelnen Tathandlungen erfasst. Insofern finden diese deliktischen Ausprägungen an dieser Stelle keine Berücksichtigung; eine nähere Betrachtung der hierzu vorliegenden statistischen Informationen erfolgt zu einem späteren Zeitpunkt.

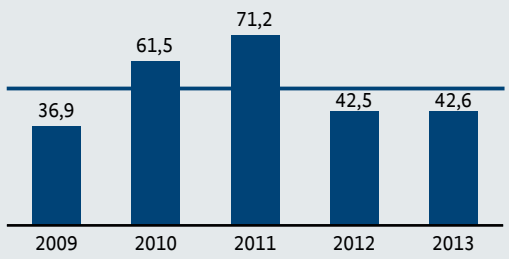
02 DoS-Angriffe belasten den Internetzugang, das Betriebssystem oder die Dienste eines Hosts mit einer größeren Anzahl Anfragen als diese verarbeiten können, woraufhin reguläre Anfragen nicht oder nur langsam beantwortet werden. Wird die Überlastung von einer größeren Anzahl anderer Systeme verursacht, so wird auch von einer verteilten Dienstblockade (Distributed Denial of Service - DDoS) gesprochen (Quelle: Wikipedia).

03 Schadprogramme, mit deren Hilfe ein Eindringling eine Zugriffs- oder Nutzungsverhinderung der Daten sowie des gesamten Computersystems erwirkt. Dabei werden Daten auf einem fremden Computer verschlüsselt oder der Zugriff auf das System wird verhindert, um für die Entschlüsselung oder Freigabe ein „Lösegeld“ zu fordern. Die Bezeichnung setzt sich zusammen aus „ransom“ (Englisch für Lösegeld) und „ware“, entsprechend dem für verschiedene Arten von Computerprogrammen üblichen Benennungsschema (Software, Malware etc.) – (Quelle: wikipedia.de).

Schäden nahezu gleichbleibend

Die für das Jahr registrierten Schäden[04] bewegen sich nahezu auf dem gleichen Niveau wie im Vorjahr. Davon entfallen rund 40 Mio. Euro auf den Bereich Computerbetrug und rund 2,6 Mio. Euro auf den Betrug mit Zugangsdaten zu Kommunikationsdiensten. 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.

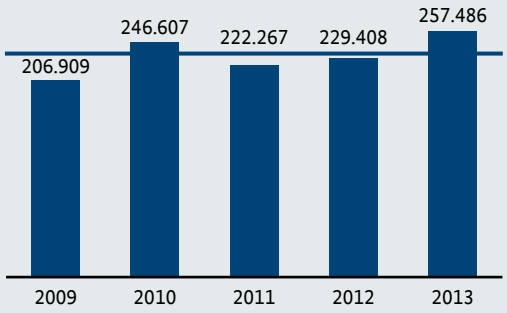
Schäden 2009 - 2013 (PKS)



Tatmittel Internet gewinnt weiter an Bedeutung

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 2009-2013 (PKS)



Auch hier zeigt die Entwicklung die weiter zunehmende Bedeutung des Internets bei der Begehung von Straftaten.

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 (E-Mail- 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) Bestandteil der digitalen Identität.

Die Täter nutzen überwiegend sogenannte „trojanische Pferde“[05], um Eingaben des Besitzers bzw. Anmeldedaten zu erlangen und Transaktionen durchführen zu können; sie gehen dabei häufig arbeitsteilig und unter Nutzung professioneller Strukturen vor. Anschließend werden die Daten entweder von den Tätern selbst eingesetzt oder aber ggf. in der Underground Economy an Dritte weiterveräußert, welche die Daten dann kriminell einsetzen. Gemäß einer repräsentativen Online-Umfage aus dem Jahr 2013[06] wurde schon rund ein Fünftel der Deutschen (21 Prozent) Opfer von Identitätsdiebstahl oder -missbrauch, weitere 27 Prozent können nicht ausschließen, dass ihre personenbezogenen Daten schon missbraucht wurden. Das Umfrageergebnis geht in seiner Dimension weit über die polizeilich registrierten Fälle des Ausspähens/Abfangens von Daten (siehe Ziffer 2.1) hinaus und ist ein weiterer Beleg für das vermutete hohe Dunkelfeld im Bereich Cybercrime.

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

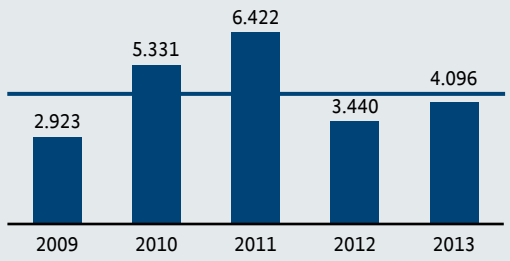
05 Ein Trojanisches Pferd, auch kurz Trojaner genannt, bezeichnet ein Computerprogramm, das als nützliche Anwendung getarnt ist, im Hintergrund aber ohne Wissen des Anwenders eine andere Funktion erfüllt. Es zählt zur Familie unerwünschter bzw. schädlicher Programme, der so genannten Malware (Quelle: wikipedia.de).

06 schufa.de (Umfrage September 2013).

Steigende Fallzahlen beim Phishing

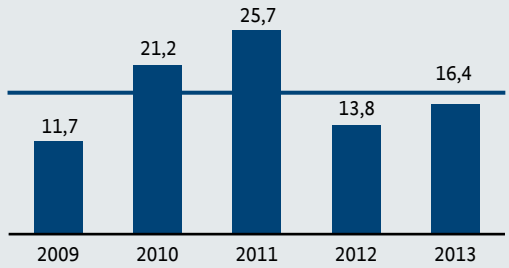
Die bekannteste Variante des digitalen Identitätsdiebstahls ist das sog. „Phishing im Zusammenhang mit Onlinebanking“. Für das Jahr 2013 wurden dem Bundeskriminalamt 4.096 Sachverhalte im Phänomenbereich Phishing gemeldet. Im Vergleich zum Jahr 2012 (3.440) bedeutet dies eine Zunahme der Fallzahlen um rund 19 %.

Fälle - Phishing im Onlinebanking 2009-2013



Nachdem u. a. durch verschiedene Schutzmaßnahmen, die verstärkte Nutzung des mTAN-Verfahrens (auch bezeichnet als smsTAN)[07] als Sicherungsmethode im Onlinebanking sowie eine noch intensivere Sensibilisierung der Anwender eine annähernde Halbierung der Fallzahlen im Jahr 2012 erreicht werden konnte, zeigt sich für das Jahr 2013 wieder ein merklicher Anstieg.
Hauptgrund hierfür dürfte sein, dass sich die Täterseite den veränderten Rahmenbedingungen technisch angepasst und neue oder verbesserte Schadsoftware entwickelt hat, um entsprechende Transaktionsverfahren zu umgehen.
Zudem sind weiterhin mehrere „Familien“ von Schadsoftware in Form von Trojanern im Umlauf, die speziell auf den deutschen Bankensektor ausgerichtet sind und über das technische Potenzial verfügen, den Endkunden mittels sog. Echtzeitmanipulation (Man-In-The-Middle/ Man-in-the-Browser-Attacken[08]) erfolgreich anzugreifen.
Insbesondere werden auch vermehrt Schadsoftwarevarianten für mobile Endgeräte festgestellt, die darauf ausgerichtet sind, mobile Transaktionssicherungsmechanismen zu umgehen. Entsprechende Schadsoftware zur Infizierung des vom jeweiligen Bankkunden genutzten mobilen Endgeräts wurde bereits am Markt platziert und ist für die meisten Betriebssysteme erhältlich. Hier zeigen sich keine grundlegenden Änderungen hinsichtlich der eingesetzten Schadsoftware gegenüber dem Vorjahr.
Diese Entwicklung zeigt einmal mehr, dass die Täterseite in der Lage ist, mit den verbesserten Sicherheitsmechanismen im Onlinebanking, wenn auch mit zeitlicher Verzögerung, Schritt zu halten.
Phishing bildet im Hinblick auf die vorhandenen Möglichkeiten und die zu erzielenden Gewinne weiterhin ein lukratives Betätigungsfeld für die Täterseite. So betrug die durchschnittliche Schadenssumme im Bereich „Phishing im Zusammenhang mit Onlinebanking“ auch im Jahr 2013 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:

Schäden - Phishing im Onlinebanking 2009-2013 (in Mio. Euro)



Zunahme digitaler Erpressungen

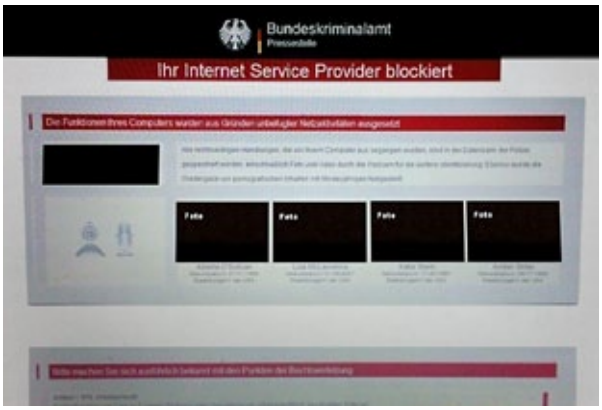
Jeder Teilnehmer der digitalen Welt (Privatperson oder Unternehmen) kann Opfer einer solchen Erpressung werden. Selbst technische Laien, die entsprechendes Equipment oder auch die gesamte „Dienstleistung“ in einschlägigen Foren der Underground Economy erwerben können, sind in der Lage, eine solche Erpressung durchzuführen.
Nach Einschätzung des BKA hat sich diese Art von Erpressung weiter ausgebreitet, insbesondere in der Ausprägung von Forderungen nach „digitalem Lösegeld“. Allein für das Jahr 2013 registrierte das BKA 6.754 Fälle von digitaler Erpressung unter Einsatz sogenannter „Ransomware“[09].

07 mTAN (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 Computerschadprogramm (zusammengesetzt aus den englischen Begriffen „Ransom“ (englisch –Lösegeld) und „Software“.

Die wohl bekanntesten Ausprägungen von Ransomware sind der sogenannte „BKA-Trojaner“ sowie der „GVU-Trojaner“[10]. Bei beiden Varianten wird dem Nutzer des



mit der Schadsoftware infizierten Computers mittels einer eingeblendeten Meldung suggeriert, dass der Computer im Zusammenhang mit verschiedenen strafbaren Handlungen in Erscheinung getreten und daher gesperrt worden ist.
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 veranlasst wird.
Technisch erfolgt bei den bekanntesten Ausprägungen von Ransomware keine Verschlüsselung der Festplatte, sondern eine Manipulation des Betriebssystems des infizierten Rechners, welche in der Folge den regulären Rechnerbetrieb verhindert. Es werden vergleichsweise geringe Forderungssummen gewählt, um möglichst viele Infektions-Opfer zu einer Zahlung zu veranlassen. Allerdings werden inzwischen auch Varianten verbreitet, bei denen tatsächlich eine Verschlüsselung der Daten erfolgt, die nur bei Zahlung aufgehoben wird. Die zu zahlenden Beträge liegen in der Regel deutlich höher.

Als technische Neuerung werden teilweise auch nicht mehr nur reine Endkundensysteme angegriffen. Mittlerweile existieren auch Varianten von Ransomware, die auf die Infektion von Server-Systemen ausgelegt sind und somit auch eine Gefahr für klein- oder mittelständische Betriebe darstellen können. Hierbei konnte festgestellt werden, dass die von den Tätern geforderten Geldbeträge höher sind als für reine Nutzersysteme.

Mittlerweile hat sich das Phänomen enorm verbreitet, angepasste Versionen der Ransomware sind weltweit im Umlauf. Dieser Umstand resultiert u. a. aus der Möglichkeit, den Quellcode des sogenannten „BKA-Trojaners“ oder sogar Komplettpakete (inklusive Hosting, Infektionen etc.) im sog. „Crime-as-a-service-Modell“ in entsprechenden Foren der Underground Economy zu kaufen.

Mobile Endgeräte – Smartphones weiterhin beliebtes Angriffsziel

Mobile Endgeräte wie Smartphones gewinnen weiterhin Marktanteile und erreichen dadurch eine immer größere Bedeutung in der digitalen Welt[11]. Die steigende Verbreitung sowie die teilweise immer noch mangelnde Sensibilität der Nutzer hinsichtlich der digitalen Gefahren im Umgang mit diesen mobilen Endgeräten sorgen für eine weiterhin hohe Attraktivität für die Täterseite. Dies zeigt sich u. a. auch in der Zunahme der für Betriebssysteme mobiler Endgeräte programmierten Schadprogramme.
Ein wesentlicher Aspekt dabei ist, dass mobile Endgeräte im Gegensatz zum klassischen PC in der Regel ständig online sind und die jeweiligen Nutzer mittlerweile einen Großteil ihrer digitalen Aktivitäten über diese Geräte abwickeln, wie Transaktionen im Bereich Onlinebanking, den Zugriff auf E-Mailkonten und soziale Netzwerke oder auch Aktivitäten im Bereich E-Commerce über entsprechende Apps.
Dazu kommt, dass auch immer mehr geschäftliche Daten über Mobilfunkverbindungen übertragen und ausgetauscht werden.

10 GVU – Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e.V.

11 Im Jahr 2013 wurden in Deutschland 26,4 Millionen Smartphones verkauft, für 2014 wird eine Absatz von rund 30 Millionen prognostiziert.

Großes Dunkelfeld

Im Bereich Cybercrime besteht ein großes Dunkelfeld. Eine Dunkelfelduntersuchung des Landeskriminalamtes Niedersachsen aus dem Jahr 2013[12] kommt zu dem Ergebnis, dass lediglich 9 % aller Delikte im Bereich Cybercrime angezeigt werden. Dieses bedeutet, bezogen auf einzelne Deliktsbereiche, dass die vorliegenden statistischen Zahlen mit dem Faktor 11 multipliziert werden müssten, um ein annähernd realistisches Bild der Cybercrime in Deutschland zu beschreiben.
Hinzu kommt, dass insbesondere bei den Deliktsfeldern Computersabotage und Datenveränderung

- 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 entstanden ist,
- 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.

Eine Aufhellung des Dunkelfeldes ist für die Strafverfolgungsbehörden jedoch sehr wichtig, um die Bekämpfung der Cybercrime zu optimieren. Ein umfassendes Bild zur Dimension und den Erscheinungsformen dieses Deliktsbereiches gibt den Strafverfolgungsbehörden die Möglichkeit, auf neue Entwicklungen schnell und zielgerichtet zu reagieren bzw. mittel- und langfristige Bekämpfungs- und Präventionsstrategien zu entwickeln. Nicht zuletzt dient dies auch der Erhöhung des Schutzes des einzelnen Nutzers von informationstechnischen Systemen.

Weiter zunehmende Professionalisierung

Unabhängig von der Entwicklung der statistischen Daten, die aufgrund des vermuteten Dunkelfeldes eine 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 Komplexität der eingesetzten Schadsoftware ablesen. 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[13] überwiegend in Form von E-Mail-Anhängen, 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[14] ohne eigentliche „Fehl-“Aktivität des Opfers statt. Eine weitere verbreitete 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.

Deepweb

Immer mehr verlagert sich der digitale Handel mit illegalen Waren und Dienstleistungen unter Nutzung der Informationstechnologien und digitaler Währungen in das sogenannte „Deepweb“, jenen Teil des Internets, der nicht über normale Suchmaschinen auffindbar ist und der als versteckter Dienst z. B. im TOR-Netzwerk[15] die Anonymität der Nutzer durch Verschleierung der Verbindungsdaten wahrt oder ein „anonymes“ Hosting ermöglicht. Über solche Online-Plattformen werden beispielsweise der illegale Handel mit Drogen, Waffen und Kreditkartendaten betrieben oder illegale Dienstleistungen, wie die Durchführung von DDoS Attacken, angeboten.

12 „Befragung zu Sicherheit und Kriminalität in Niedersachsen“, Landeskriminalamt Niedersachsen, November 2013.

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

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

15 Netzwerk zur Anonymisierung von Verbindungsdaten, dass u. a. für Web-Browsing genutzt werden kann. TOR schützt seine Nutzer vor der Analyse des Datenverkehrs.

3 GESAMTBEWERTUNG

Das Phänomen Cybercrime nimmt in der polizeilichen Aufgabenwahrnehmung eine immer größere Rolle ein. Dabei entgrenzt das Internet die Kriminalität in nahezu allen Deliktsbereichen und bietet zugleich durch die Anwendung der zahlreich vorhandenen Verschlüsselungs- und Anonymisierungsmöglichkeiten eine geeignete Plattform zur Vorbereitung und Begehung von Straftaten.
Die bereits in den Vorjahren festgestellte Veränderung der erkannten Täterstrukturen hat sich im Berichtsjahr fortgesetzt. Die Täter begehen heute nicht mehr nur die Straftaten im eigentlichen Sinne, sondern bieten auch 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. Es agieren daher nicht mehr nur hoch spezialisierte Einzeltäter mit umfassenden IT-Kenntnissen, sondern vermehrt auch Kriminelle ohne spezifische Fachkenntnisse, die für die Begehung der Straftaten arbeitsteilig zusammenwirken.
Insoweit ist das Profil der im Bereich Cybercrime agierenden Straftäter heterogen bei gleichzeitig hohem Innovationspotenzial. Hinsichtlich der Motivation spielen neben monetären Gründen auch ideologische und politische Ziele eine Rolle.

Cyberkriminelle sind hoch flexibel, suchen nach immer neuen Einfallstoren und nutzen sich bietende technische Möglichkeiten für ihre Zwecke. Dabei reagieren sie sehr schnell auf neue Sicherheitsstandards, wie z. B. beim Phishing im Onlinebanking.
Jeder kann Opfer werden, sei es der einzelne Bürger, Unternehmen oder auch staatliche Stellen. Proportional mit der Zunahme der Bedeutung der IT als Bestandteil des Alltags der Bürger steigen die Manipulations- und Angriffsmöglichkeiten auf Seiten der Cyberkriminellen.
Cyberkriminelle handeln global, nationale Grenzen spielen keine Rolle, wobei Tatorte, Taterfolgsorte und Aufenthaltsort der Täter völlig unabhängig voneinander zu sehen sind.
Die von den verschiedenen Facetten des Phänomens Cybercrime ausgehenden Gefahren dürften in ihrem Ausmaß und in ihren Ausprägungen weiter zunehmen. So weist der im Januar 2014 bekannt gewordene Diebstahl von 16 Millionen E-Mail-Adressen exemplarisch auf die Schadensdimensionen im Phänomen der Cybercrime hin. Die Bekämpfung von Cybercrime im Sinne eines ganzheitlichen Ansatzes, d. h. im Verbund der zuständigen Sicherheitsbehörden unter Einbeziehung der Privatwirtschaft, muss daher sowohl im nationalen als auch im internationalen Kontext intensiviert werden.

IMPRESSUM

Herausgeber
Bundeskriminalamt
SO 51
65173 Wiesbaden

Stand
2013

Druck
BKA

Bildnachweis
Fotos: Polizeiliche Quellen

www.bka.de