Bundeskriminalamt

CYBERCRIME

Bundeslagebild 2011

BKA

CYBERCRIME
Bundeslagebild 2011

Bundeskriminalamt
65173 Wiesbaden

www.bka.de

INHALTSVERZEICHNIS

1 VORBEMERKUNG

Der Begriff Cybercrime umfasst alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik (IuK) oder gegen diese begangen werden. Das Lagebild Cybercrime behandelt spezielle Phänomene und Ausprägungen dieser Kriminalitätsform, bei denen Elemente der elektronischen Datenverarbeitung (EDV) wesentlich für die Tatausführung sind (Cybercrime im engeren Sinne).

Das Lagebild informiert zu den Entwicklungen im Berichtszeitraum und beschreibt das Gefahren- und Schadenspotenzial dieser Kriminalitätsform und deren Bedeutung für die Kriminalitätslage in Deutschland.

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

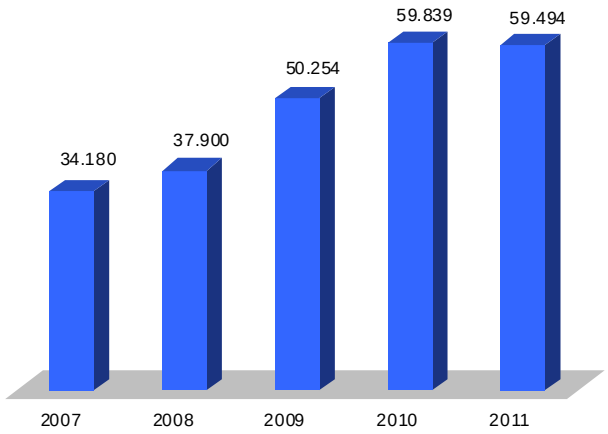
2 DARSTELLUNG UND BEWERTUNG DER KRIMINALITÄTSLAGE

2.1 Polizeiliche Kriminalstatistik

2.1.1 Gesamtentwicklung

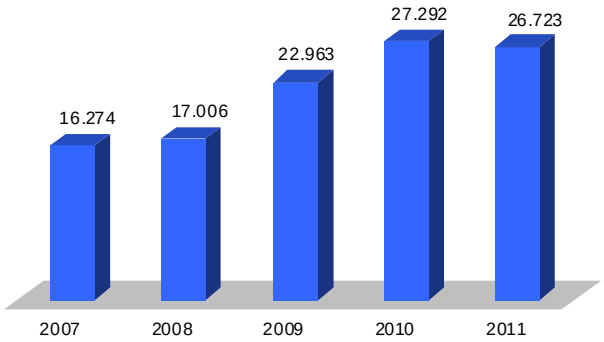
Die Zahl der in der PKS erfassten Fälle von Cybercrime, also aller Straftaten, die unter Ausnutzung moderner Informations- und Kommunikationstechnik oder gegen diese begangen wurden, ging im Jahr 2011 auf 59.494 Fälle zurück. Dies entspricht einem geringfügigen Rückgang von rund 0,6 % gegenüber dem Vorjahr.

Cybercrime im engeren Sinne 2007-2011 (PKS)[1]



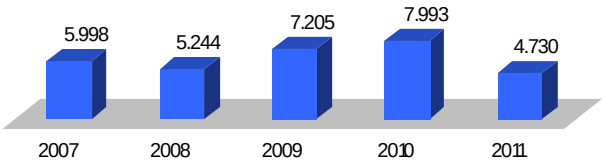
Eine Betrachtung der einzelnen Deliktsbereiche ergibt im Fünf-Jahres-Vergleich folgendes Bild:

Computerbetrug 2007-2011 (PKS)

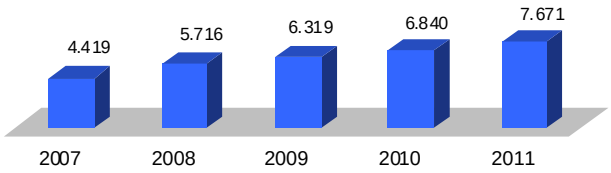


[1] Umfasst die Delikte: Computerbetrug (PKS 517500), Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten (PKS 517900), Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung (PKS 543000), Datenveränderung/Computersabotage (PKS 674200) sowie Ausspähen, Abfangen von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

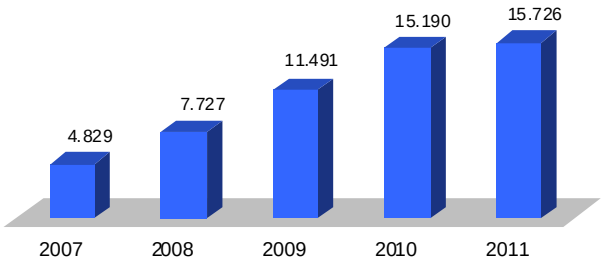
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten 2007-2011 (PKS)



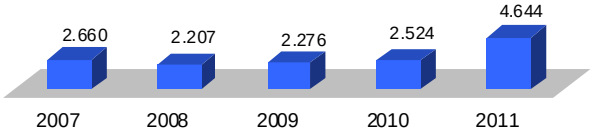
Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung 2007-2011 (PKS)



Ausspähen/Abfangen von Daten 2007-2011 (PKS)

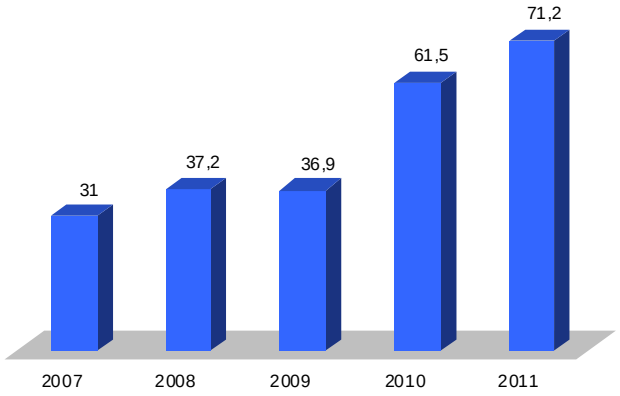


Datenveränderung, Computersabotage 2007-2011 (PKS)



Die mit Abstand größte Straftatengruppe ist der Computerbetrug mit einem Anteil von rund 45 % aller Fälle. Deutliche Veränderungen zeigen sich in den Deliktsbereichen Datenveränderung/Computersabotage (+84 %), Datenfälschung, Täuschung im Rechtsverkehr bei Datenverarbeitung (+12 %) sowie beim Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten (-41 %).

Schäden 2007 - 2011 (in Mio. Euro)



Bei den registrierten Schäden ist ein Anstieg um rund 16 % auf rund 71,2 Mio. Euro zu verzeichnen (2010: 61,5 Mio. Euro). Davon entfallen rund 50 Mio. Euro auf den Bereich Computerbetrug und rund 21,2 Mio. Euro auf den Betrug mit Zugangsdaten zu Kommunikationsdiensten[2].

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.

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, Straftaten im Zusammenhang mit gezielten DDoS-Attacken[3] oder auch die vielfältigen Ausprägungen der digitalen Erpressung, werden in der PKS nicht unter dem Begriff Cybercrime, sondern vielmehr unter den PKS-Schlüsseln der einzelnen Tathandlungen erfasst. Dies führt dazu, dass keine auf validen Daten basierenden Aussagen zum tatsächlichen Ausmaß in diesen von den Strafverfolgungsbehörden als relevant wahrgenommenen Segmenten des Bereichs Cybercrime möglich sind.

---

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

[3] 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.

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

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

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[4] überwiegend in Form von E-Mailanhängen, 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[5] ohne eigentliche 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.

Zusätzlich dazu hat sich im Bereich der sog. Underground Economy[6] auch in Deutschland eine breite Szene etabliert, die sich zuvor überwiegend in englisch- oder russischsprachigen Foren und Plattformen betätigte.

Diese Feststellungen resultieren aus der Auswertung des kriminalpolizeilichen Meldedienstes, des polizeilichen Informationsaustausches auf nationaler und internationaler Ebene sowie der Analyse von öffentlich zugänglichen Quellen. Nur auf diesem Wege kann, natürlich auch unter Einbeziehung entsprechender Daten aus der PKS, eine realistische Bewertung von qualitativen Veränderungen im Bereich Cybercrime erfolgen.

---

4 Computerschadprogramm (zusammengesetzt aus den englischen Begriffen „**mal**icious“ (bösartig) und „Soft**ware“**)

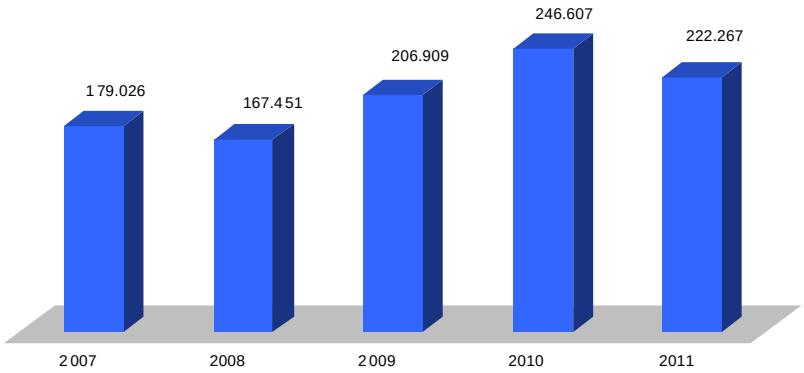
5 Bezeichnet das unerwünschte Herunterladen von Schadsoftware allein durch das Anschauen einer dafür präparierten Webseite (engl. Drive-by: im Vorbeifahren)

6 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.

2.1.2 Tatmittel Internet

Zur Abrundung des Gesamtbildes muss über die Betrachtungen der reinen Fallzahlen von Cybercrime hinaus auch ein Blick auf das Internet als Tatmittel geworfen werden. Zwar lassen sich aus diesen Zahlen keine konkreten Aussagen bezogen auf den Bereich Cybercrime treffen, letztlich zeigen sie aber, welche Bedeutung das Internet in den letzten Jahren im Hinblick auf die Begehung von Straftaten gewonnen hat.

Tatmittel Internet 2007-2011 (PKS)



2.2 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 wie z. B. ICQ und Skype, soziale Netzwerke wie Stayfriends, Facebook usw.),
- E-Commerce (Onlinebanking, Onlinebrokerage, internetgestützte Vertriebsportale aller Art wie z. B. eBay oder Buchungssysteme für Flüge, Hotels, Mietwagen usw.),
- 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 dieser digitalen Identität.

Die Täter im Bereich Cybercrime sind an allen Arten und Ausprägungen von digitalen Identitäten interessiert, die sie in ihren kriminellen „Geschäftsmodellen“ verwenden können. Der Diebstahl digitaler Identitäten ist für Kriminelle äußerst lukrativ. Alle Arten digitaler Identitäten (z. B. Bankaccounts, Accounts für soziale Netzwerke, Kreditkartendaten) werden in den illegalen Webshops der sogenannten Underground Economy angeboten. Gerade im Bereich des digitalen Identitätsdiebstahls ist von einem großen Dunkelfeld auszugehen. In diesem Bereich wissen die Geschädigten in aller Regel nicht, dass ihre Rechner infiziert und verschiedene Bestandteile ihrer digitalen Identität entwendet wurden. Erst dann, wenn es zu einem missbräuchlichen Einsatz kommt, der zumeist mit einem finanziellen Verlust einhergeht, erfolgt unter Umständen eine Mitteilung an die Strafverfolgungsbehörden.

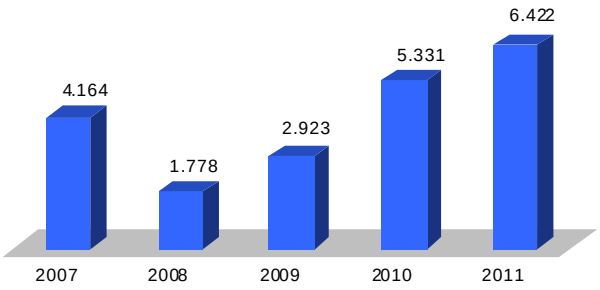
In der Realität ist es aber häufig so, dass z. B. Banken, Kreditkartenunternehmen oder große Online-Unternehmen wie eBay oder PayPal ihre Kunden zwar auf die vorliegende Infektion hinweisen, die Konten sperren und gegebenenfalls bereits eingetretene Schäden ersetzen, die Kunden aber nicht auf die Möglichkeit hinweisen, eine Strafanzeige zu erstatten.

2.2.1 Phishing

2.2.1.1 Fall- und Schadenszahlen

Die bekannteste Variante des digitalen Identitätsdiebstahls ist das sogenannte Phishing im Zusammenhang mit Onlinebanking. Für das Jahr 2011 wurden dem Bundeskriminalamt 6.422 Sachverhalte im Phänomenbereich Phishing gemeldet. Im Vergleich zum Jahr 2010 bedeutet dies einen Anstieg der Fallzahlen um mehr als 20 %.

Fälle - Phishing im Onlinebanking 2007-2011



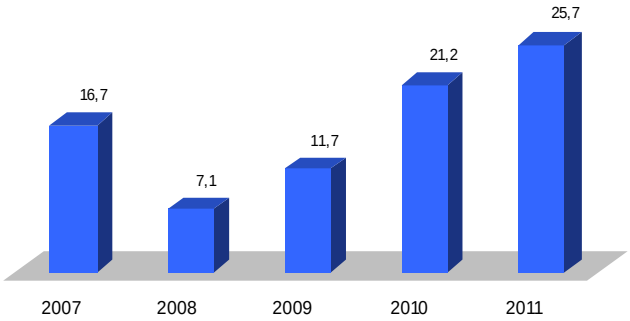
Der seit dem Jahr 2008 festgestellte Trend steigender Fallzahlen in diesem Bereich hat sich weiter bestätigt. Der rasante Anstieg der Fälle in den letzten drei Jahren zeigt die enorme Anpassungsfähigkeit der Täterseite auf die Einführung neuer technischer Sicherungen[7] sowie das täterseitig vorhandene technische Know-how zur Überwindung solcher Sicherungsmechanismen.

Phishing bildet im Hinblick auf das vorhandene Schadenspotenzial und die Lukrativität für die Täterseite weiterhin einen Schwerpunkt im Bereich Cybercrime. So betrug die durchschnittliche Schadenssumme im Bereich Phishing im Zusammenhang mit Onlinebanking im Jahr 2011 rund 4.000 Euro pro Fall. Auf

[7] Flächendeckende Einführung des iTAN – Verfahrens im Jahr 2008: (iTAN - indizierte Transaktionsnummer - Einmalpasswort zur Legitimation einer Transaktion im Onlinebanking)

dieser Berechnungsgrundlage ergeben sich unter Berücksichtigung der dem Bundeskriminalamt in den letzen vier Jahren gemeldeten Fallzahlen folgende ungefähre Schäden:

Schäden - Phishing im Onlinebanking 2007-2011 (in Mio. Euro)



Hinsichtlich der im Bereich des Phishing im Onlinebanking täterseitig eingesetzten Schadsoftware gibt es keine grundlegend neuen Erkenntnisse. Aktuell sind weiterhin 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[8] mittels sog. Echtzeitmanipulation (Man-In-The-Middle/Man-in-the-Browser-Attacken[9]) erfolgreich anzugreifen.

So wurden unter anderem zunehmend Fälle des Computerbetruges im Onlinebanking bekannt, bei denen die Täterseite mittels „klassischen Phishings“ die Zugangsdaten von Bankkunden für das Onlinebanking ausspäht, ohne Wissen des Bankkunden das mTAN-Verfahren einrichtet und eine täterseitig verwendete Mobilfunknummer zum Empfang der mTAN hinterlegt. Der durch das Geldinstitut per Briefpost zugestellte Aktivierungscode für das mTAN-Verfahren wird sodann von der Täterseite (beispielsweise durch Entwendung des Briefes aus dem Briefkasten) abgefangen.

2.2.1.2 Infektionswege

Abgesehen von einigen in wenigen Einzelfällen festgestellten speziellen Varianten kristallisieren sich folgende Methoden als die von der heutigen Phisher-Generation bevorzugten Modi Operandi zur Verbreitung der Schadsoftware heraus:

- „Drive-by-Infection“
  Unerwünschtes Herunterladen der Schadsoftware allein durch Aufruf einer von der Täterseite präparierten Webseite,

---

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

[9] Bei einer „Man-In-The-Middle-Attacke“ steht der Angreifer entweder physikalisch und 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.

- „Soziale Netzwerke“
  Verteilung der Schadsoftware über Soziale Netzwerke (z. B. Facebook, Studi-VZ, Wer-Kennt-Wen), in denen das (spätere) Opfer dem Täter („Freund“) vertraut und dann gutgläubig infizierte Anhänge öffnet bzw. entsprechenden Links folgt (die dann zur Infektion des Opfersystems führen),
- „Spear-Infection“
  Gezielte Kontaktaufnahme zu bestimmten Personen mittels persönlich adressierter Phishing- oder Infektionsmails, um auf diesem Wege in den Besitz der zur Durchführung weiterer Aktionen erforderlichen Daten zu gelangen bzw. den Rechner des Opfers zu infizieren. Ein Grund für die Nutzung dieses Modus Operandi besteht darin, dass viele Internetnutzer bei ungewollt erhaltenen anonymen E-Mails zunehmend skeptisch reagieren und vorsichtiger geworden sind, jedoch bei persönlich an sie adressierten E-Mails weniger sensibel reagieren.

2.2.2 Digitale Erpressung

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“. Bei dieser Erpressungsmethode erfolgt die Manipulation des Rechners des Opfers mittels Malware[10] in Form von sog. Ransomware[11], wodurch der Nutzer nicht mehr frei über seinen Rechner verfügen kann. Ihm wird eine Benutzeroberfläche eingeblendet, welche ihn über die Sperrung des Rechners sowie die Entsperrungsmöglichkeit in Form der Zahlung eines bestimmten Geldbetrages informiert.

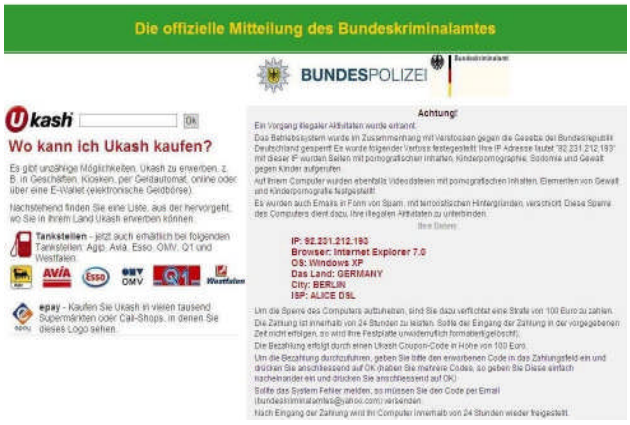


Abb. 1 – „BKA-Trojaner“

Eine bekannte Variante der derzeit im Internet kursierenden Ausprägungen von Ransomware ist der sogenannte „BKA-Trojaner“. Hier 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 sei. Die Meldung informiert den

[10] Computerschadprogramm (zusammengesetzt aus den englischen Begriffen "**mal**icious" (bösartig) und "Soft**ware**")

[11] Ransom (englisch) – Lösegeld.

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. Dem Geschädigten wird angedroht, dass er bei ausbleibender Zahlung mit vollständigem und unwiderruflichem Datenverlust zu rechnen habe.

Technisch erfolgt 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.

Neben dem „BKA-Trojaner“ existieren weitere Abwandlungen dieser Ransomware, wobei die Logos von Microsoft Windows, der GEMA[12] oder der GVU[13] verwendet werden.

Neben dieser Variante bedient sich die Täterseite überwiegend folgender weiterer Modi Operandi zur Durchsetzung von „Lösegeldforderungen“ im Zuge der Nutzung gestohlener Daten oder unrechtmäßig erworbener Zugriffsberechtigungen:

- Digitales Schutzgeld
  Die Erpressung von Schutzgeld erfolgt in den bisher bekannt gewordenen Fällen durch Drohung der Durchführung von DDoS-Angriffen auf die IT-Infrastruktur von Unternehmen. Bei Ablehnung der Forderungen erfolgen tatsächlich entsprechende Attacken in Form einer durch den angegriffenen Webserver nicht mehr zu verarbeitenden Anzahl technisch sinnloser Anfragen. Diese Anfragen gehen in aller Regel von mittels Schadsoftware kompromittierten und so übernommenen PC (sog. Bots)[14] aus. Zahlt das Erpressungsopfer den geforderten Betrag, so enden die Angriffe bzw. werden die Webpräsenzen des Opfers von Angriffen (dieses Angreifers) verschont.
- Rückkauf kompromittierter Daten
  Kompromittierte Daten, die dem ursprünglichen Berechtigten „gestohlen“ wurden, werden durch den Angreifer (Hacker) zum Rückkauf angeboten.
- Schweigegeldforderung
  Der Angreifer droht damit, den erfolgreichen Angriff auf die Daten bzw. IT-Infrastruktur eines Unternehmens publik zu machen. Das betroffene Unternehmen wird aufgefordert, diese Veröffentlichung gegen Zahlung eines entsprechenden Geldbetrages abzuwenden.

[12] Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte

[13] Gesellschaft zur Verfolgung von Urheberrechtsverletzungen

[14] Siehe Ziffer 2.4 „Bot-Netze“

2.2.3 Carding

In diesem Phänomenbereich erfolgt oftmals eine Zweiteilung der eigentlichen Tatausführung. Am Anfang steht der „Datendieb und/oder -händler“, welcher die Kreditkartendaten entweder mittels Einsatz von Schadsoftware beim Opfer abgreift oder über den unbefugten Zugriff auf ungenügend gesicherte und nicht verschlüsselte Datenbanken erlangt. Anschließend werden diese für monetäre Vorteile jeglicher Art nutzbaren Kreditkartendaten über Webportale und Foren der Underground Economy weiter veräußert.

An dieser Stelle greift der zweite Teil der Tatausführung (das eigentliche Carding), wo nun die „gekauften“[15] Kreditkartendaten zum Onlinekauf von Waren genutzt und diese Waren anschließend z. B. über eBay oder durch die Täterseite selbst betriebene Webshops weiterverkauft werden.

Hier liegt die Besonderheit des Carding, denn in aller Regel erfolgen keine direkten Online-Vermögensverfügungen anhand der ausgespähten oder entwendeten Kreditkartendaten, vielmehr generieren sich die monetären Vorteile auf der Täterseite aus dem Weiterverkauf der mittels der Kartendaten unrechtmäßig erlangten Waren.

Zum Carding liegen keine validen Lagedaten vor. Der Grund hierfür dürfte sein, dass der Kartenemittent den durch den missbräuchlichen Einsatz von Kartendaten entstandenen finanziellen Schaden im Regelfall ersetzt und somit der Karteninhaber keinen Grund für eine Anzeigenerstattung sieht.

2.3 Mobile Endgeräte - Smartphones

Mobile Endgeräte wie Smartphones stellen weiterhin ein interessantes Zielfeld für die Täter dar, allein aufgrund der Tatsache, dass sich diese Geräte deutschland- und weltweit immer weiter verbreiten.[16] Hinzu kommt, dass die Einsatzgebiete von Smartphones im täglichen Gebrauch zunehmend vielfältiger werden, z. B. im Bereich Onlinebanking zur Autorisierung von Transaktionen oder zum unmittelbaren Zugriff auf E-Mailkonten und Konten sozialer Netzwerke über entsprechende Apps. [17]

Folgende Aspekte einer täterseitigen Nutzung dieser Geräte sind aus hiesiger Sicht von besonderer Bedeutung:

- SMS-basierte Authentifizierungsverfahren

  Hierbei infiziert die Täterseite mobile Endgeräte mit Schadsoftware[18], um SMS-basierte Transaktionssicherungssysteme zu kompromittieren. Dabei bestehen Einsatzmöglichkeiten insbesondere im Bereich des Onlinebankings sowie des Einsatzes von Kreditkarten im Internet. Die

---

15 Preis für einen Datensatz: 3-5 Euro (Durchschnittswert)

16 Im Jahr 2011 wurden in Deutschland 10 Millionen Smartphones verkauft (Quelle: www.bitkom.org).

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

18 Bei der eingesetzten Schadsoftware handelte es sich um eine Variante des ZeuS-Trojaners, der zu den leistungsfähigsten Arten von Schadsoftware zählt.

Täter leiten SMS mit mobilen TAN an ein eigenes Mobiltelefon oder entsprechende Datentransferdienste um.

Beispielhaft wird hier folgernder Modus Operandi erwähnt: Durch die Täterseite erfolgt eine Infektion des Computers des Geschädigten. Dadurch erlangt diese die Zugangsdaten zum Onlinebanking-Account (und weitere Ausprägungen der digitalen Identität). Zusätzlich erfolgt mittels Social Engineering[19] eine Infektion des genutzten Smartphones. Daran anschließend veranlasst die Täterseite z. B. eine Transaktion im Onlinebanking. Die Bank verschickt daraufhin eine SMS an die im Onlinebankingkonto hinterlegte Rufnummer (die Rufnummer des Geschädigten). Die SMS geht zwar auf dem Handy des Opfers ein, wird durch die Schadsoftware auf dem Mobiltelefon jedoch unterdrückt und entweder mittels SMS oder Datentransferdienst an von den Tätern genutzte Ressourcen weitergeleitet. Diese gelangen damit in den Besitz der Transaktionsnummer und können die Zahlungsverfügung, in diesem Fall die Onlinebanking-transaktion, entsprechend authentifizieren.

- Handy-Botnetze

  Die mittlerweile hohen Verbindungsraten und leistungsfähigen Prozessoren machen Smartphones für Bot-Herder[20] attraktiv. Dies rührt daher, dass Mobiltelefone in der Regel ständig online sind und somit für ein Botnetz[21] ständig zur Verfügung stehen. Im Gegensatz dazu wird der klassische PC in der Regel nach Gebrauch ausgeschaltet, wodurch er dann nicht mehr für ein Botnetz genutzt werden kann. Zusätzlich können die im Zusammenhang mit Botnetzen bekannten Modi Operandi auch mit „Handy-Botnetzen“ realisiert werden.

2.4 Botnetze

Wie in den Jahren zuvor bedienten sich die Täter auch im Jahr 2011 bei der Tatausführung sogenannter Botnetze. Dabei werden zahlreiche per Schadcode infizierte Computer ohne Wissen ihrer Besitzer über sogenannte Command- & Control-Server (C&C-Server) ferngesteuert. Der physische Standort sowie die Identität der Straftäter sind oftmals nicht zu ermitteln. Die Aufspielung des Schadcodes erfolgt analog zum Phishing. Diese Schadsoftware erlaubt dem Täter einen nahezu vollständigen Zugriff auf den Computer des Opfers.

Botnetze und ihre Kapazitäten stellen nach wie vor eine weltweit lukrative Handelsware im Bereich der Underground Economy dar. Die Bot-Herder vermieten Bots, durch die mittels DDoS-Attacken gezielte Angriffe auf die Server z. B. eines Unternehmens durchgeführt werden. Dabei werden die Server einer Flut von Anfragen ausgesetzt, was dazu führt, dass das System nicht mehr in der Lage ist, diese Flut zu bewältigen und zusammenbricht. Gerade bei Unternehmen, deren Geschäftstätigkeit Dienstleistungen

---

[19] Bezeichnet eine Art sozialer Manipulation, mittels derer der Täter durch zwischenmenschliche Beeinflussung das Opfer dahingehend zu beeinflussen versucht, dass dieses vertrauliche Informationen preisgibt oder vom Täter vorgegebene Handlungen durchführt.

[20] Herder (englisch) – Hirte

[21] Siehe Ziffer 2.4 „Bot-Netze“

oder den Handel von Produkten über das Internet umfasst, können Nichterreichbarkeiten von Vertriebsportalen zu schwerwiegenden wirtschaftlichen Nachteilen führen. In diesem Zusammenhang sind Botnetze auch als Infrastruktur für tradierte Kriminalitätsformen, wie z. B. Erpressungen, nutzbar.

Seriöse Angaben zur Gesamtzahl der weltweit in Botnetzen zusammengeschlossenen Rechner sind weiterhin nicht oder nur sehr lückenhaft möglich. Die Sicherheitsbehörden können zwar immer wieder einzelne Erfolge bei der Bekämpfung dieser Netze aufweisen[22], letztendlich kann dieses Phänomen aber nur in Form einer verstärkten internationalen Zusammenarbeit zwischen den Sicherheitsbehörden und den weltweit agierenden IT-Unternehmen erfolgversprechend bekämpft werden.

[22] Z. B. Zerschlagung des Botnetzes „Coreflood“ durch das FBI. „Coreflood“ bestand seit 2002 und umfasste rund zwei Millionen Rechner.

3. GESAMTBEWERTUNG UND AUSBLICK

Das Gefährdungs- und Schadenspotenzial des Phänomens Cybercrime ist unverändert hoch. Weiterhin werden neben den Zugangsdaten im Bereich des Onlinebankings alle Formen und Arten der digitalen Identität ausgespäht und illegal eingesetzt.

Die aus Sicht des BKA zunehmende Fokussierung auf das Zielfeld „Mobile Endgeräte“ zeigt, dass auch die Täterseite die sich ergebenden Tatgelegenheiten, sei es in der Verwendung als Teil eines Botnetzes oder auch beim Diebstahl aller Arten von Daten, erkannt hat und zur Begehung von Straftaten weiter nutzen wird. Zwar liegen hierzu aktuell keine belastbaren Zahlen vor, jedoch ist vor dem Hintergrund steigender Nutzerzahlen im Bereich „Mobile Endgeräte“ mit einer Zunahme der Fallzahlen zu rechnen.

Das Phänomen Cybercrime entwickelt sich weiterhin dynamisch. Sicherheitsmaßnahmen werden sehr schnell durch geeignete Schadsoftware überwunden. Die Dynamik lässt sich am Beispiel des Phishing im Onlinebanking eindrucksvoll darstellen. Wurde durch die Einführung des Sicherungsverfahrens iTAN im Jahr 2008 noch ein kurzzeitiger Rückgang der Fallzahlen erreicht, so haben sich seither die Fallzahlen verdreifacht. Gerade in diesem Bereich ist auch in den nächsten Jahren mit weiterhin steigenden Fallzahlen zu rechnen, vor allem vor dem Hintergrund, dass die Täterseite schon jetzt über das entsprechende technische Wissen zur Umgehung moderner Sicherungssysteme wie das mTAN-Verfahren verfügt und dieses Know-how erfolgreich einsetzt. Dieses Beispiel unterstreicht die Anpassungs- und Innovationsfähigkeit der Täter im Bereich Cybercrime.

Die bereits in den Vorjahren festgestellte Veränderung der erkannten Täterstrukturen hat sich im Berichtsjahr fortgesetzt. Es agieren nicht mehr nur hochspezialisierte Einzeltäter mit einem entsprechenden umfassenden IT-Hintergrundwissen, sondern vermehrt auch Kriminelle ohne spezifische Fachkenntnisse, die für die Begehung der Straftaten arbeitsteilig zusammenwirken. Dies zeigt sich darin, dass Täter heute teilweise nicht mehr nur selbst die Straftaten im eigentlichen Sinne begehen, sondern vielmehr auch die zur Begehung von Straftaten erforderlichen Schadprogramme oder gar komplette kriminelle Infrastrukturen in den einschlägigen Foren der Underground Economy global zum Kauf oder zur Miete anbieten. Dabei sind die angebotenen Werkzeuge aufgrund ihrer relativ einfachen Handhabung auch für Täter ohne fundierte IT-Spezialkenntnisse nutzbar.

Die von den verschiedenen Facetten des Phänomens Cybercrime ausgehenden Gefahren sind in ihrem Ausmaß und in ihren Ausprägungen allerdings nur schwer zu bewerten. Nach Einschätzung des BKA wird der Bereich Cybercrime auch in den kommenden Jahren ein weiter wachsendes Problem darstellen, welchem die Sicherheitsbehörden sowohl präventiv als auch repressiv weiterhin entschlossen entgegenwirken müssen.

Bundeskriminalamt

65173 Wiesbaden

www.bka.de