Bundeskriminalamt

CYBERCRIME

Bundeslagebild 2010

BKA

CYBERCRIME
Bundeslagebild 2010

Bundeskriminalamt

65173 Wiesbaden
info@bka.bund.de
www.bka.de

1 VORBEMERKUNG 5

2 DARSTELLUNG UND BEWERTUNG DER KRIMINALITÄTSLAGE 6

2.1 Polizeiliche Kriminalstatistik 6

2.2 Diebstahl digitaler Identitäten 8

2.2.1 Phishing 9

2.2.2 Digitale Erpressung 10

2.2.3 Carding 12

2.3 Mobile Endgeräte - Smartphones 12

2.4 Botnetze 13

3. GESAMTBEWERTUNG UND AUSBLICK 14

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).

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

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 2010 auf 59.839 Fälle (2009: 50.254 Fälle). Dies entspricht einem Anstieg von rund 19 % gegenüber dem Vorjahr.

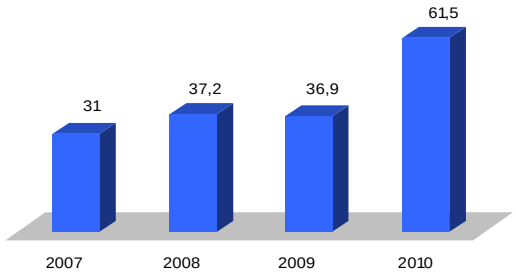
Die Anzahl der polizeilich registrierten Straftaten ist in allen Straftatengruppen gestiegen. Dabei bilden erneut die Fälle der Straftatengruppe Computerbetrug mit einem Anteil von rund 46 % (27.292 Fälle) die mit Abstand größte Gruppe; das Fallaufkommen ist gegenüber dem Jahr 2009 um rund 19 % gestiegen.

Straftaten (-Gruppen)	Jahr 2010	Jahr 2009	Veränderung -absolut-	Veränderung -in %-
Computerbetrug	27.292	22.963	4.329	18,9
Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	**7.993**	**7.205**	**788**	**10,9**
Datenfälschung, Täuschung im Rechtsverkehr bei Datenverarbeitung	6.840	6.319	521	8,2
Datenveränderung/Computersabotage	**2.524**	**2.276**	**248**	**10,9**
Ausspähen/Abfangen von Daten	15.190	11.491	3.699	32,2
Cybercrime im engeren Sinne	**59.839**	**50.254**	**9.585**	**19.1**

Bei den registrierten Schäden ist ein enormer Anstieg um mehr als 66 % gegenüber dem Jahr 2009 zu verzeichnen. So beläuft sich der im Jahr 2010 registrierte Schaden aller in der PKS mit Schadenssumme erfassten Delikte aus dem Bereich Cybercrime[1] auf insgesamt rund 61,5 Mio. Euro (2009: 36,9 Mio. Euro), wobei rund 47 Mio. Euro auf den Bereich Computerbetrug und 14,5 Mio. Euro auf den Bereich Betrug mit Zugangsdaten zu Kommunikationsdiensten entfallen.

[1] Erfassung der Schadenssumme erfolgt lediglich bei den Delikten Computerbetrug (PKS-Schlüssel 517500) und Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten (PKS-Schlüssel 517900)

Schäden 2007 - 2010 (in Mio. Euro)



Eine Bewertung des Phänomens Cybercrime allein auf Basis statistischer Zahlen ist nicht möglich. Einzelne bzw. besonders relevante Phänomene der Cybercrime, wie z. B. Phishing im Bereich Onlinebanking oder auch Straftaten im Zusammenhang mit gezielten DDos-Attacken[2] auf Server eines Unternehmens oder einer Behörde, werden in der PKS nicht unter dem Begriff Cybercrime erfasst. Vielmehr erfolgt eine statistische Erfassung dieser Delikte unter den PKS-Schlüsseln der einzelnen Tathandlungen. Dies führt dazu, dass keine auf validen Daten basierenden Aussagen zum tatsächlichen Ausmaß gerade in diesen als von den Strafverfolgungsbehörden als relevant wahrgenommenen Segmenten des Bereichs Cybercrime möglich sind.

Zusätzlich ist, insbesondere bei den Deliktsfeldern Computersabotage und Datenveränderung, von einem großen Dunkelfeld auszugehen. Dies ist unter anderem darauf zurückzuführen, dass

⇒ Straftaten häufig durch den Geschädigten gar 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,

⇒ aufgrund immer weiter verbreiteter technischer Sicherungseinrichtungen eine große Anzahl der Straftaten 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 sowie der festgestellten zunehmenden Spezialisierung und Professionalisierung der Täter ablesen. Darüber hinaus hat sich mittlerweile im Bereich der sog. Underground Economy[3] auch in Deutschland eine breite Szene etabliert, die sich zuvor überwiegend in englisch- oder russischsprachigen Foren und Plattformen betätigte.

---

[2] 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.

[3] 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 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 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).

Darüber hinaus sind auch alle anderen zahlungsrelevanten Informationen (insbesondere Kreditkartendaten einschließlich der Zahlungsadressen sowie weiterer Informationen) ebenfalls Bestandteil dieser digitalen Identität.

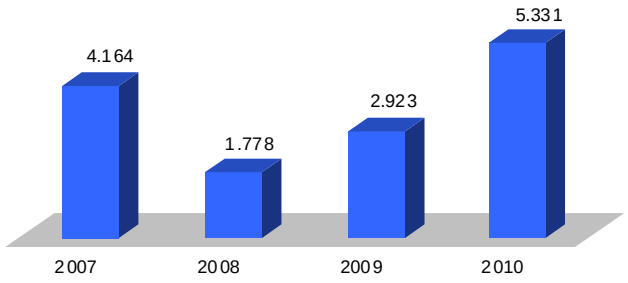
Abb. 1 – Startseite eines Undergroundshops

Die Täter im Bereich Cybercrime sind an allen Arten und Ausprägungen von digitalen Identitäten interessiert, die sie in ihren der aktuellen Situation angepassten 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, wobei genauere Aussagen hierzu aufgrund unzureichender Daten nicht möglich sind. In diesem Bereich wissen die Geschädigten in aller Regel nicht, dass ihre Rechner infiziert und verschiedene Bestandteile ihrer digitalen Identität entwendet wurden. Nur dann, wenn es zu einem missbräuchlichen Einsatz kommt, erfolgt unter Umständen eine Mitteilung an die Strafverfolgungsbehörden.

2.2.1 Phishing

Die wohl bekannteste Variante des digitalen Identitätsdiebstahls ist das sogenannte Phishing im Zusammenhang mit Onlinebanking. Für das Jahr 2010 wurden dem Bundeskriminalamt 5.331 Sachverhalte im Phänomenbereich Phishing gemeldet. Im Vergleich zum Jahr 2009 (2.923 Fälle) bedeutet dies einen Anstieg der Fallzahlen um mehr als 82 %.

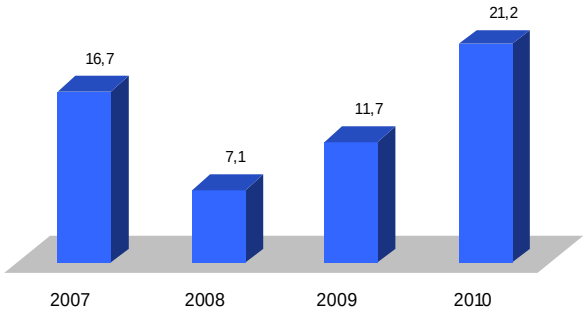
Fälle - Phishing im Onlinebanking 2007-2010



Damit hat sich der bereits Ende 2008 einsetzende Trend zu steigenden Fallzahlen in diesem Bereich bestätigt. Die flächendeckende Einführung des iTan-Verfahrens[4] hatte zwar im Jahr 2008 die erhoffte Wirkung in Bezug auf sinkende Fallzahlen entfaltet, jedoch zeigt der rasante Anstieg der Fallzahlen in den letzten beiden Jahren die Anpassungsfähigkeit der Täterseite auf die Einführung neuer technischer Sicherungsmechanismen.

Phishing ist weiterhin als einer der Schwerpunkte im Bereich Cybercrime anzusehen, sowohl im Hinblick auf das festgestellte Schadenspotenzial als auch in Bezug auf die Lukrativität für die Täterseite. So betrug die durchschnittliche Schadenssumme im Bereich Phishing im Zusammenhang mit Onlinebanking im Jahr 2010 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 2007-2010 (in Mio. Euro)



Zum Phänomen „Phishing beim Online-banking“ ist anzumerken, dass aufgrund der Erfahrungen der vergangenen Jahre davon ausgegangen werden kann, dass dem Bundeskriminalamt jeweils lediglich ungefähr 40 % der tatsächlichen Fälle bekannt wurden. Somit dürften die tatsächlichen Fallzahlen und der tatsächliche Schaden wesentlich höher liegen.

[4] iTAN – indizierte Transaktionsnummer (Einmalpasswort zur Legitimation einer Transaktion im Onlinebanking)

Nach aktueller Erkenntnislage sind mehrere „Familien“ von Schadsoftware in Form von Trojanern im Umlauf, die speziell auf den deutschen Bankenmarkt ausgerichtet sind und über das technische Potential verfügen, das iTAN-Verfahren mittels sog. Echtzeitmanipulation (Man-In-The-Middle/Man-in-the-Browser-Attacken[5]) erfolgreich anzugreifen.

Die Phisher-Generation von heute bedient sich bei der Verbreitung der Schadsoftware zudem immer verfeinerterer Varianten. Mittlerweile wird der weitaus größte Teil der Schadsoftware mittels „Drive-by-Infection“[6] verbreitet. Die Gefahr, den eigenen Computer durch den bloßen Aufruf von Webseiten zu infizieren, ist größer denn je und wächst weiter. Eine weitere Variante ist die Verteilung der Schadsoftware über Soziale Netzwerke (z. B. Facebook, Studi-VZ, Wer-Kennt-Wen), wo das (spätere) „Opfer“ dem Täter („Freund“) vertraut und dann gutgläubig entsprechend infizierte Anhänge öffnet bzw. entsprechenden Links folgt (die dann zur Infektion des Opfers führen). Nach wie vor werden jedoch auch die sogenannte „Spear-Infections“ von Täterseite eingesetzt, also das gezielte Anschreiben bestimmter Personen mit 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 mehr oder minder 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

Eine sich zunehmend verbreitende Variante aus dem Bereich des Diebstahls digitaler Identitäten ist die digitale Erpressung. Dabei benutzt die Täterseite entweder gestohlene Daten oder durch Infizierungen von Rechnern erworbene Zugriffsberechtigungen zur Durchsetzung von „Lösegeldforderungen“. Jeder Teilnehmer der digitalen Welt, unabhängig ob Privatperson oder Unternehmen, wird hierdurch zum potenziellen Erpressungsopfer, erpressbar selbst durch den technischen Laien, der entsprechendes Equipment oder auch die gesamte „Dienstleistung" in einschlägigen Foren der Underground Economy erwerben kann. Zur näheren Erläuterung hier einige der in diesem Zusammenhang bekannt gewordenen Ausprägungen:

- 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

[5] 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.

[6] Eine durch einen Anwender aufgerufene Internetseite enthält ein sog. „iFrame“, das im Hintergrund - für den Anwender unsichtbar und ohne dass eine Benutzeraktion notwendig wäre - ein Schadprogramm von einem anderen Server lädt und anschließend auf dem dadurch infizierten Rechner ausführt. Dabei werden häufig Sicherheitslücken im Webbrowser ausgenutzt.

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) [7] aus. Zahlt das Erpressungsopfer den geforderten Betrag, so enden die Angriffe bzw. werden die Webpräsenzen des Opfers von Angriffen (dieses Angreifers) verschont.

- Digitales Lösegeld

Mittels Malware[8] in Form von sog. Ransomware[9] wird der Rechner derart manipuliert, dass der Nutzer nicht mehr frei über seinen Rechner verfügen kann. Ihm wird eine Benutzeroberfläche eingeblendet, welche ihn über die Rechnerinfektion und eine angebliche bösartige Verschlüsselung der Festplatte informiert. Gleichzeitig wird der Nutzer aufgefordert, eine bestimmte Webseite zu besuchen, auf welcher nach Zahlung eines Betrages im unteren dreistelligen Bereich in Form von uKash oder PaysafeCard-Credits (anonyme digitale Zahlungsmittel im Sinne eines digitalen Bargeldes) ein individueller Code zur Entschlüsselung des infizierten Rechners erlangt werden könne. Dem Geschädigten wird angekündigt, dass er bei ausbleibender Zahlung mit vollständigem und unwiderruflichem Datenverlust zu rechnen habe. Technisch erfolgt keine Verschlüsselung der Festplatte, sondern eine Manipulation des Master Boot Record[10] des infizierten Rechners, welche in der Folge den regulären Rechnerbetrieb verhindert. Es werden vergleichsweise geringe Forderungssummen gewählt, um einen möglichst großen Anteil der Infektions-Opfer zur Durchführung einer Zahlung zu bewegen (möglichst geringe Hemmschwelle).

- 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.

---

7 Siehe Ziffer 2.4

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

9 Ransom (englisch) – Lösegeld.

10 Bei dem Master Boot Record (MBR) handelt es sich um den ersten Datenblock auf der Festplatte, der für das Laden (Booten) vorhandener Betriebssysteme auf dem Rechner verantwortlich ist.

2.2.3 Carding

Beim sogenannten Carding erfolgen in aller Regel keine direkten online-Vermögensverfügungen anhand ausgespähter oder entwendeter Kreditkartendaten. Die Kreditkartendaten werden in diesen Fällen missbräuchlich dazu genutzt, um zunächst online Waren zu kaufen, die anschließend z. B. über eBay oder eigene (scheinbar legale) Webshops weiterverkauft werden.

Auch in diesem Bereich liegen keine validen Lagedaten vor[11], jedoch deuten die Informationen aus dem nationalen und internationalen polizeilichen Informationsaustausch darauf hin, dass die Fallzahlen und die daraus resultierenden Schäden im vergangenen Jahr deutlich gestiegen sind. Dabei zeigt sich eine Verschiebung vom Card-Present- zum „eCommerce-Bereich“[12], da die illegal erlangten Kartendaten immer seltener zur Herstellung sog. „white plastics“[13], sondern direkt für die Abwicklung von online-Käufen eingesetzt werden.

Durch den weit verbreiteten Einsatz von Schadsoftware werden von der Täterseite über das Internet massenhaft einsetzbare Kreditkartendaten abgegriffen und auf Servern gespeichert. Über Webportale und Foren der Underground Economy findet ein schwunghafter Handel mit widerrechtlich erlangten Kreditkartendaten statt. Durch die hohe Verfügbarkeit von validen Kreditkartendaten entwickelt sich der Handel mit illegal erlangten Kreditkartendaten zu einem Massenphänomen.

2.3 Mobile Endgeräte - Smartphones

Mittlerweile geraten auch mobile Endsysteme ins Zielspektrum der Täter, wobei sie den Versuch unternehmen, parallel zum Computer auch Mobiltelefone (Smartphones) zu infizieren, um an die Daten möglicher SMS-basierter Authentifizierungsverfahren zu gelangen. Im September 2010 wurden erste Versuche des Infizierens mobiler Endgeräte mit Schadsoftware registriert.[14] In der Vergangenheit sind zumindest zwei Varianten von Schadsoftware aufgetreten, die bei Kunden bestimmter Institute anschließend eine Infizierung von Mobiltelefonen versuchten.
Die Täter können derart infizierte Mobiltelefone dazu nutzen, SMS-basierte Transaktionssicherungssysteme zu kompromittieren. Dabei bestehen Einsatzmöglichkeiten insbesondere im Bereich des Onlinebankings sowie des Einsatzes von Kreditkarten im Internet. Die Täter leiten SMS mit mobilen TAN-Nummern an ein eigenes Mobiltelefon oder entsprechende Datentransferdienste um. Dadurch werden betrügerische Transaktionen initiiert und mittels einer zuvor an das infizierte mobile

---

11 Grund hierfür dürfte sein, dass der Kartenemittent den durch den missbräuchlichen Einsatz der Kartendaten entstandenen finanziellen Schaden im Regelfall ersetzt und somit der Karteninhaber keinen Grund für eine Anzeigeerstattung sieht.

12 Bei Card-Present Transaktionen liegt dem Händler die Kreditkarte physisch vor, während im Bereich eCommerce lediglich die Kartendaten zur Durchführung der Transaktionen übermittelt werden.

13 Gefälschte Kreditkarten.

14 Bei der eingesetzten Schadsoftware handelte es sich um eine Variante des ZeuS-Trojaners, der zu den leistungsfähigsten Arten von Schadsoftware zählt und auch das deutsche Onlinebanking attackiert. Bisher wurde diese ZeuS-Variante in Spanien, der Türkei und Polen festgestellt.

Endgerät übermittelten SMS autorisiert. Auf diese Weise können SMS-basierte Schutzmechanismen von Kreditkartenunternehmen, wie der Versand einer SMS nach einer erfolgten Transaktion, durch Unterdrückung der SMS überwunden werden.

2.4 Botnetze

Wie in den Jahren zuvor bedienten sich die Täter auch im Jahr 2010 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.

Seriöse Angaben zur Gesamtzahl der weltweit in Botnetzen zusammengeschlossenen Rechner sind nur sehr schwer möglich. Zur Veranschaulichung der Dimension sei an dieser Stelle das Botnetz Mariposa[15] genannt, welches Anfang 2010 durch die spanische Polizei in Zusammenarbeit mit dem FBI zerschlagen werden konnte. Allein dieses Botnetz umfasste rund 12 Millionen Rechner. Laut einer Studie[16] liegt Deutschland, bezogen auf die Anzahl der in Bots zusammengeschlossenen Computer, weltweit auf dem dritten Rang hinter den USA und China.

Botnetze und ihre Kapazitäten stellen nach wie vor eine weltweit lukrative Handelsware im Bereich der Underground Economy dar. Sogenannte „Herder“ (Hirten) 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 oder der 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, zu verstehen.

[15] Mariposa (spanisch) – Schmetterling

[16] IT-Sicherheitsunternehmen Trend Micro.

3. GESAMTBEWERTUNG UND AUSBLICK

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

Das Phänomen Cybercrime entwickelt sich aktuell 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 dürfte auch in den nächsten Jahren mit weiterhin steigenden Fallzahlen zu rechnen sein, vor allem vor dem Hintergrund, dass die Täterseite schon jetzt über das entsprechende technische Wissen zu verfügen scheint, auch mobile Sicherungssysteme anzugreifen.

Gerade die beginnende Fokussierung auf das Zielfeld “Mobile Endgeräte“ zeigt, dass auch die Täterseite die aus der zunehmenden weltweiten Verbreitung dieser Geräte 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 nutzen will.

Dieses Beispiel unterstreicht die Anpassungs- und Innovationsfähigkeit der Täter im Bereich Cybercrime. Die erkannten Täterstrukturen haben sich verändert. Es agieren nicht mehr wenige hochspezialisierte Straftäter, sondern überwiegend Kriminelle, die zumeist auf internationaler Ebene arbeitsteilig zusammenwirken. Dies zeigt sich auch darin, dass die 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.

65173 Wiesbaden

info@bka.de

www.bka.de