Cybercrime in Österreich

Report 2013

.BK BUNDESKRIMINALAMT

Impressum:
Herausgeber: Bundeskriminalamt
Josef-Holaubek-Platz 1, 1090 Wien
Grafiken und Fotos: © Bundeskriminalamt, © Europol,
© Interpol; **Druck:** Digitaldruckerei des Bundesministeriums
für Inneres, Herrengasse 7, 1010 Wien
Stand: August 2014

Inhaltsverzeichnis

Vorwort

Liebe Leserinnen und Leser!

Die Welt ist permanent im Umbruch und dies in einer nie zuvor da gewesenen Geschwindigkeit. Das digitale Zeitalter hat aufgrund seiner technologischen Entwicklungen alle Bereiche des täglichen Lebens weltumspannend revolutioniert. Und diese Dynamik nimmt weiter zu. Technologisierung und Internationalisierung werden weiter die bestimmenden Einflussgrößen unserer gesellschaftlichen Entwicklung sein. In gleichem Maße, wie sich die Gesellschaft und ihre Technologien verändern, sind auch Kriminalitätsphänomene einem steten Wandel unterworfen. Aktuell prägen die technologischen Entwicklungen einer digitalisierten Welt die Erscheinungsformen der heutigen Kriminalität – das gilt im Besonderen für das Kriminalitätsphänomen Cybercrime.

Cybercrime präsentiert sich heute als rein internationale Kriminalitätsform. Organisierte Tätergruppen bedienen sich modernster Technologien und verlegen dadurch auch die Tatorte von der physisch greifbaren in die virtuelle Welt. Auch bei den Opfern gibt es Veränderungen. Durch moderne intensive Social-Media-Kommunikation werden insbesondere junge Menschen immer häufiger Opfer von Cybercrime.

Cybercrime zählt seit Jahren zu den wachsenden illegalen Wirtschaftszweigen. Immer stärkere Verflechtungen des geschäftlichen und gesellschaftlichen Lebens mit dem Internet sowie die scheinbar unaufhaltsame Einbindung der oftmals überforderten Bürgerinnen und Bürger in den virtuellen Cyber-Raum sind die Ursachen für neue Bedrohungen. Diese stellen Behörden, Institutionen und Unternehmen vor große Herausforderungen, da moderne Wirtschaftskriminalität heutzutage quasi rund um die Uhr im Internet stattfindet. Die Schäden für die betroffenen Unternehmen und Volkswirtschaften gehen in astronomische Höhen. Finanztransaktionen und damit die Verschleierung oder Vernichtung wichtiger Beweismittel können von versierten Kriminellen in Sekundenbruchteilen durchgeführt werden, wobei die klassischen kriminalgeografischen Räume durch den virtuellen Raum entgrenzt werden. Der Aktionsraum der Täter ist per Mausklick weltumspannend.

Cybercrime bietet heute ein breites Spektrum von Tätergruppierungen: Junge Einzeltäter, sogenannte „Scriptkiddies", die sich – da sie ihren Opfern nicht mehr gegenübertreten müssen – in Ermangelung psychologischer Hemmschwellen als Hacker versuchen. Oder hoch professionelle Schadcodeprogrammierer, die in professionell agierenden kriminellen Organisationen arbeiten. Beide Beispiele verbildlichen das aktuelle Täterspektrum. Die sogenannte „Underground Economy" steht den „Cybercrime-Anfängern" ebenso wie den „Profis" quasi als Online-Selbstbedienungsladen 24/7 zur Verfügung. Das Internet stellt das erforderliche fachliche Know-how, Tatbegehungsmittel für alle erdenklichen Zwecke und nicht zuletzt ein unüberschaubares Netzwerk von professionell miteinander in Verbindung stehenden Berufsverbrechern bereit.

Auch die sich immer schneller verändernde neue Sprache mit immer spezifischerem Fachvokabular, die die Kriminellen für ihre Machenschaften benutzen, erschweren neben Verschlüsselungs- und

Anonymisierungssoftware die Gefahrenabwehr und die Strafverfolgung durch die Sicherheits- und Justizbehörden. Diesen vielfältigen Bedrohungsphänomenen des digitalen Zeitalters muss durch die internationale Gemeinschaft der Rechtsstaaten begegnet werden.

Deshalb ist es gerade auch für die Prozessarchitektur der Sicherheitsbehörden, die mit der Bekämpfung von Cybercrime beauftragt sind, notwendig, sich an die sich stetig verändernden Bedingungen durch kreative und effektive Lösungsmodelle anzupassen, um mit der Innovationsgeschwindigkeit des modernen Technologiefortschrittes mithalten und den damit einhergehenden veränderten Kriminalitätsformen begegnen zu können.

Der Cybercrime-Report 2013 soll hierfür einen Beitrag leisten. Unser Bemühen war es, aktuelle Entwicklungen, Phänomene, Herausforderungen und mögliche Tendenzen in diesem wichtigen Kriminalitätsfeld verständlich zu erklären und auf diese Weise zu einer Erhöhung des Sicherheitsbewusstseins im Deliktsfeld Internetkriminalität beizutragen.

Mag.ª Johanna Mikl-Leitner
Bundesministerin für Inneres

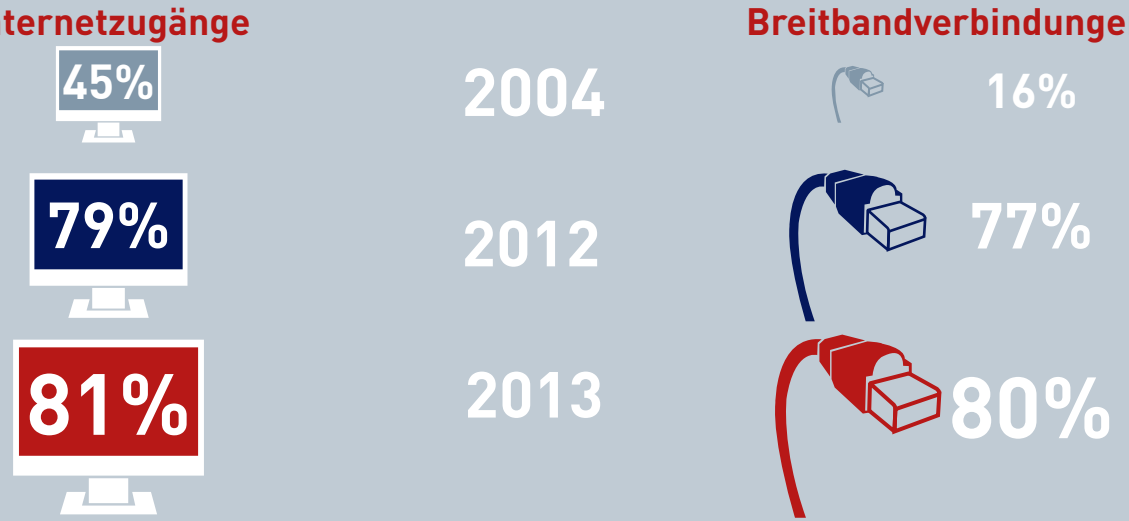
General Franz Lang
Direktor des Bundeskriminalamts

Die Ausgangslage: Der Einsatz von Informations- und Kommunikationstechnologie (IKT) in Österreich

Das Internet und mit ihm die gesamte Technologiebranche im Bereich Informations- und Kommunikationstechnologie hat in den letzten 20 Jahren einen revolutionären Wandel für das tägliche Leben aller mit dieser Hochtechnologie täglich in Interaktion stehenden Gesellschaften bewirkt. Das gilt für das Privatleben ebenso wie für die Unternehmens- und Geschäftswelt der führenden Industrienationen. Nicht umsonst spricht man heute treffend vom digitalen Zeitalter, in das die Menschheit eingetreten ist.

IKT-Technologien haben heute per Mausklick allgegenwärtigen Einfluss auf unser Leben. In Österreich verfügten im Jahr 2013 81 Prozent der privaten Haushalte über einen Internetzugang. 83 Prozent der Bevölkerung benützen regelmäßig einen Computer bzw. eine IKT-Technologie. In der Altersgruppe der 16- bis 24-Jährigen sind es sogar über 99 Prozent.

Anteil der Haushalte mit Internetzugang und Bereitbandverbindungen in Österreich



Quelle: Statistik Austria

Gerade für die jungen Bevölkerungsgruppen sind die neuen Kommunikationsformen über Smartphone oder Tablet im Wege der Nutzung von Social-Media-Plattformen wie Facebook oder Twitter sowie von Chat-Applikationen wie WhatsApp, Messenger usw. Bestandteil ihrer Kommunikationskultur geworden. Das Einstiegsalter für Internetnutzung bei Kindern und Jugendlichen sinkt weiter. Die Vielfalt von Risiken und Bedrohungen für Internet-User wächst kontinuierlich an und beschränkt sich nicht allein auf Gefahren, die sich gegen das Vermögen von Personen oder Unternehmen richten, wie etwa die bekannten Betrugsdelikte beispielsweise im bargeldlosen Zahlungsverkehr, die Kriminelle über Internetanwendungen begehen. Entsprechend der praktischen Durchdringung von IKT-Technologien in allen Lebensbereichen haben sich auch die Bedrohungsbilder weiterentwickelt, wobei hier dem Zuwachs im Bereich der Nutzung von Mobile Devices große Bedeutung zukommt. 2013 nutzten 63 Prozent aller Internetnutzerinnen und -nutzer in Österreich tragbare Geräte (Mobiltelefone, Smartphones, Laptops und Tablets) für den mobilen Internetzugang. Der Umstand, dass immer mehr Kriminelle die Möglichkeiten dieser multifunktionalen Geräte für die Begehung ihrer Straftaten einsetzen, bewirkt, dass diese mobilen IKT-Technologien auch in der polizeilichen Arbeit immer stärker an Bedeutung gewinnen.

98 Prozent der Unternehmen in Österreich hatten im Jahr 2013 einen Internetzugang und 86 Prozent verfügten über eine unternehmenseigene Website. Im IKT-Branchensektor sowie im Bereich Reparatur von Datenverarbeitungs- und Telekommunikationsgeräten waren es 100 Prozent der in diesem Wirtschaftszweig tätigen Unternehmen.

Im Jahr 2013 verfügten 97 Prozent der 30.224 Klein- und mittelständischen Unternehmungen (KMU) – also Unternehmen mit zehn bis 49 Beschäftigten – bereits über einen Internetzugang und 84 Prozent über eine eigene Firmenwebsite. Präventionsmaßnahmen sowie sicherheitsbehördliche Informations- und Aufklärungsarbeit für die sichere Anwendung moderner IKT-Technologien erlangen in Anbetracht dieser statistischen Zahlenwerte insbesondere für die KMU in Österreich große Bedeutung.

Strafrecht

Cybercrime ist als Querschnittsmaterie zu sehen und erfordert somit auch einen breiten Ansatz zu deren Bekämpfung. Das Budapester Übereinkommen vom 23. November 2001 dient hierfür als Grundlage, indem es nicht nur „klassische" Kriminalität (Cybercrime im weiteren Sinn) wie etwa „Straftaten mit Bezug zu Kinderpornografie" oder „computerbezogenen Betrug" auflistet sondern auch Cybercrime im engeren Sinn umfasst, das sind kriminelle Handlungen gegen die Netzwerke selbst, gegen Geräte in diesen Netzwerken oder gegen Dienste und Daten in diesen Netzwerken.

Im Strafgesetzbuch (StGB) finden sich diese Bedrohungen im Bereich der allgemeinen Kriminalität unter Nutzung von Informations- und Kommunikationstechnik wieder. Hier werden jene Delikte angeführt, bei denen Elemente der elektronischen Datenverarbeitung in den Tatbestandsmerkmalen enthalten sind, wie zum Beispiel Datenbeschädigung (§ 126a StGB), Hacking (§ 118a StGB), DDoS-Attacken (§ 126b StGB) usw., sowie andererseits auch jene Straftaten, bei denen die Informations- und Kommunikationstechnik zur Ausführung der Tat eingesetzt wird. Wie zum Beispiel beim Betrug (§ 146ff StGB) oder bei der Kinderpornografie im Internet (§ 207a StGB). Cybercrime als Querschnittmaterie kann daher in einer Vielzahl von Bereichen und Varianten in Erscheinung treten. Deshalb ist es auch notwendig, im Bereich des Strafrechts aktuellen Entwicklungen Rechnung zu tragen. So ist etwa „Cybergrooming" seit Jänner 2012 strafbar (§ 208a StGB).

Trends und Entwicklungen

Neben den Deliktsfeldern der Betrugs- und Finanzmittelkriminalität, der Verbreitung von Kinderpornografie, der Suchtgiftkriminalität und dem „Enabling Factor" für Terrorismus konnten im Jahr 2013 folgende aktuelle Trends im Bereich Cybercrime festgestellt werden:

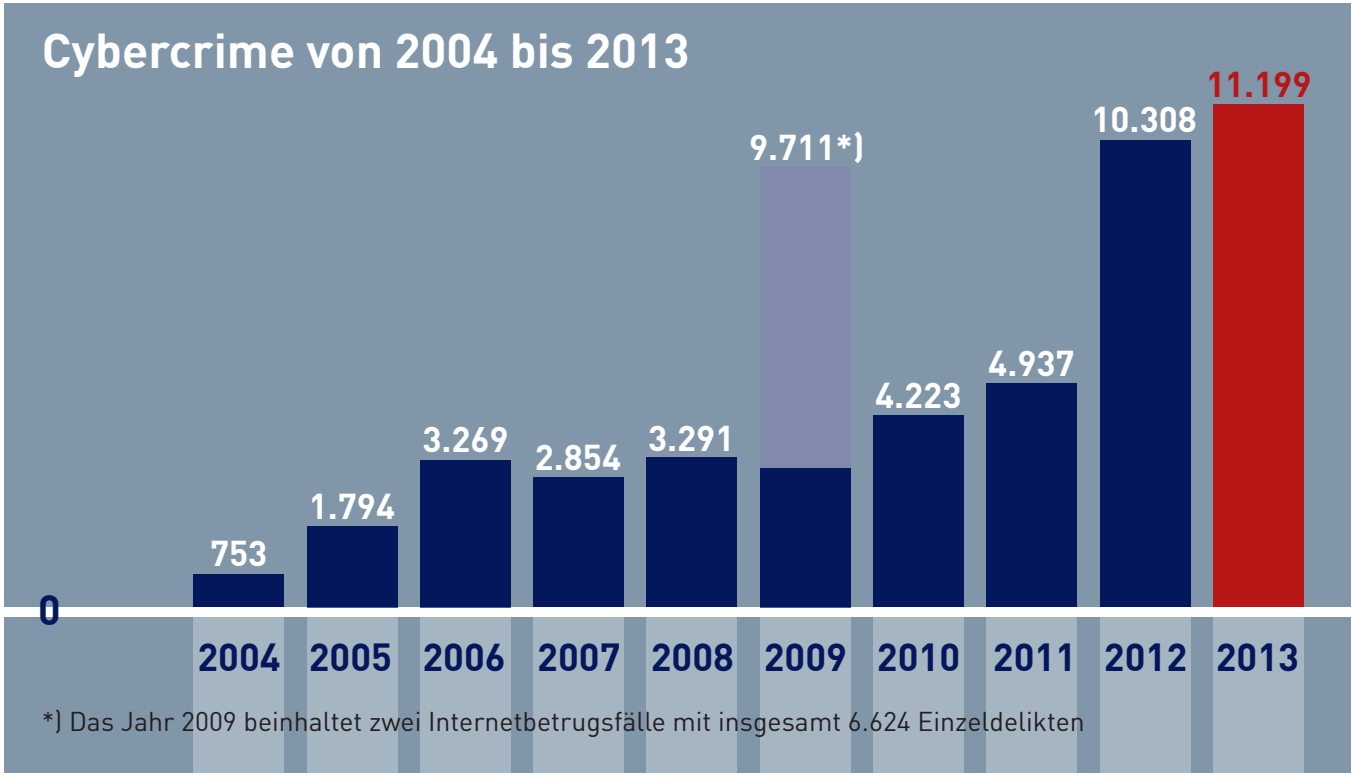
- die ungezielte Verteilung von Schadsoftware mit dem Fokus auf Identitätsdiebstahl,
- die Schadsoftwareinfiltration beim Internetsurfen mit dem Ziel die Kontrolle über die jeweiligen Rechner zu übernehmen,
- das gezielte Hacking von Webservern, um dort Schadsoftware zu platzieren und
- mehrstufige Angriffe, bei denen zum Beispiel Sicherheitsdienstleister oder zentrale Zertifizierungsstellen kompromittiert werden, um in weiteren Schritten die eigentlichen Ziele anzugreifen

Im Jahr 2013 war weltweit neuerlich ein starker Anstieg der auf Mobiltelefone ausgerichteten Schadsoftware feststellbar. Außerdem spezialisieren sich Cyberkriminelle immer stärker auch auf soziale Netzwerke und verwenden diese für Betrugsversuche oder die Verbreitung von Schadsoftware. Auch die Zahl der Betrugshandlungen im Internet stieg 2013 weiter an.

Die Motive für viele Cyberdelikte sind vor allem finanzielle Interessen sowie Langeweile und Geltungsdrang. Darüber hinaus hat das Phänomen des „Hacktivismus", mit dem Ziel mediale Aufmerksamkeit zu erreichen, als Motivationsgrund an Bedeutung gewonnen. Cyberdelikte werden zunehmend von organisierten Banden begangen. Diese haben sich auf individuelle Bereiche spezialisiert und bieten ihre Dienstleistungen auf einschlägigen Märkten an. Das Ausmaß des Schadens, der durch Cyber-Kriminelle verursacht wird, lässt sich nur schwer erfassen. Viele Betroffene erstatten keine Anzeige bei der Polizei, da die Schadenssumme oft unterhalb der Anzeigenschwelle liegt und sie der Meinung sind, dass die Täter ohnedies nicht ausgeforscht werden können. Zahlreiche geschädigte Personen oder Firmen haben außerdem kein Interesse daran, eventuelle Schwachstellen in ihrem System im Zusammenhang mit Cyber-Attacken bekannt zu machen.

Cyber-Kriminalität – Statistik

Auch 2013 gab es einen weiteren Anstieg der IT-Kriminalität im Netz – jedoch nicht mehr in den Ausmaßen wie in den Vorjahren. 2013 wurden 11.199 Fälle von Cybercrime angezeigt. Das entspricht einem Anstieg von 8,6 Prozent gegenüber 2012.

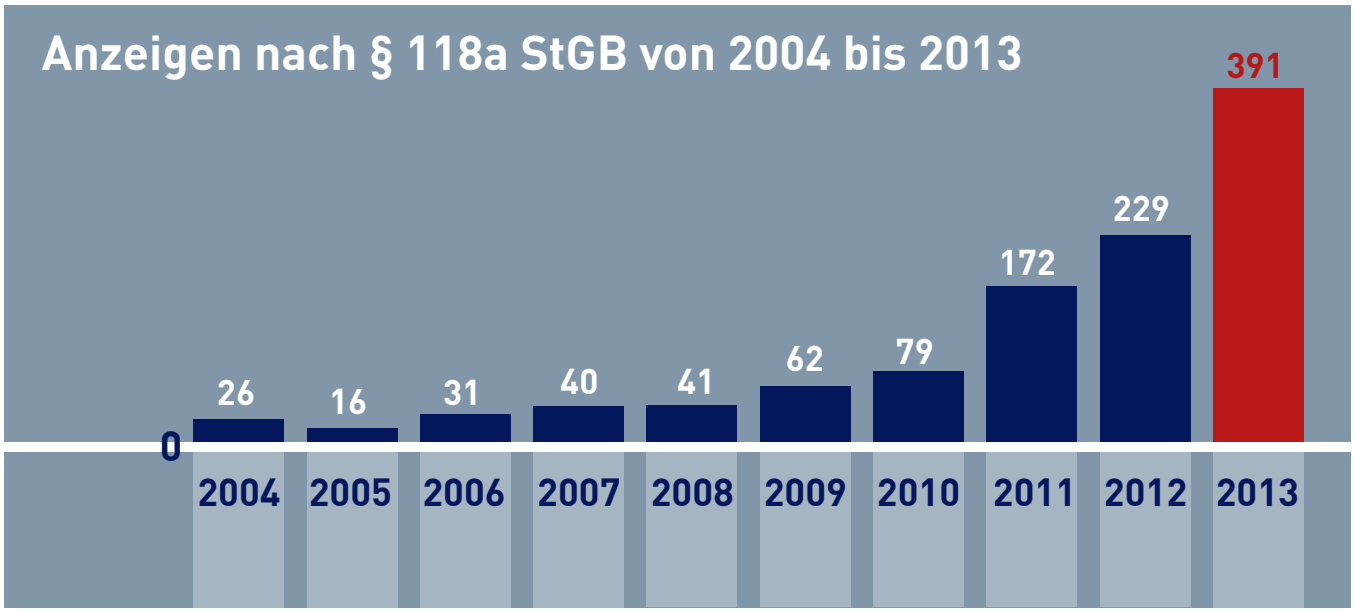


Die Aufklärungsquote bei allen Cybercrime-Delikten betrug 2013 40,7 Prozent, um 13,5 Prozent mehr als 2012.

Bei den reinen IT-Delikten (Cybercrime im engeren Sinn) sank die Aufklärungsquote um 2,3 Prozent von 20,1 auf 17,8 Prozent. Dies ist unter anderem auf die immer stärkere Professionalisierung der international vernetzen Tätergruppierungen zurückzuführen.

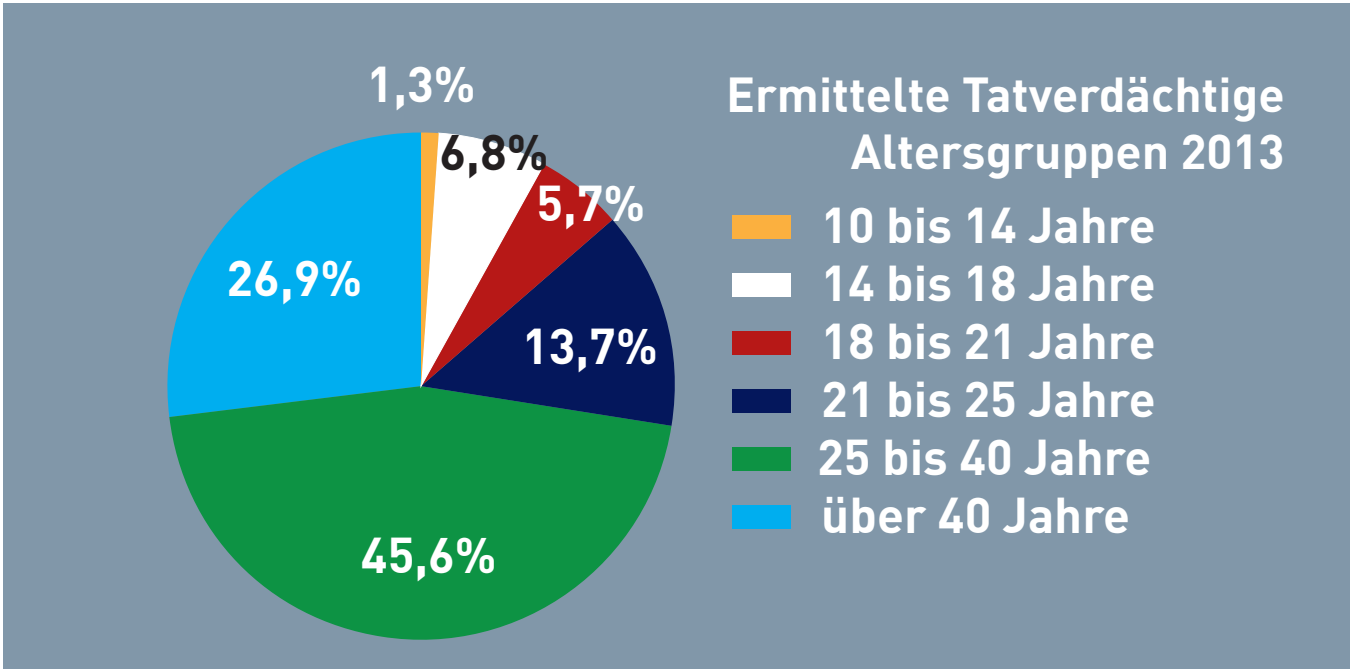
Die Zahl der angezeigten Cybercrime-Delikte im engeren Sinn sank 2013 um 23 Prozent. So wurden beispielsweise 421 Datenverarbeitungsmissbrauchsfälle nach § 148a StGB angezeigt. 2012 waren es 806 Fälle, was einem Rückgang um 47 Prozent entspricht. Dieser Rückgang ist unter anderem auf das weitgehend zyklische Auftreten von Phishing- und Malware-Attacken zurückzuführen.

Im 10-Jahresvergleich ergeben sich für Cybercrime-Delikte bereichsübergreifend besonders hohe Zuwachsraten. Die Zahl der Anzeigen nach § 118a StGB (Widerrechtlicher Zugriff auf ein Computersystem) stieg von 26 auf 391, was einem Anstieg von mehr als 1.400 Prozent entspricht.

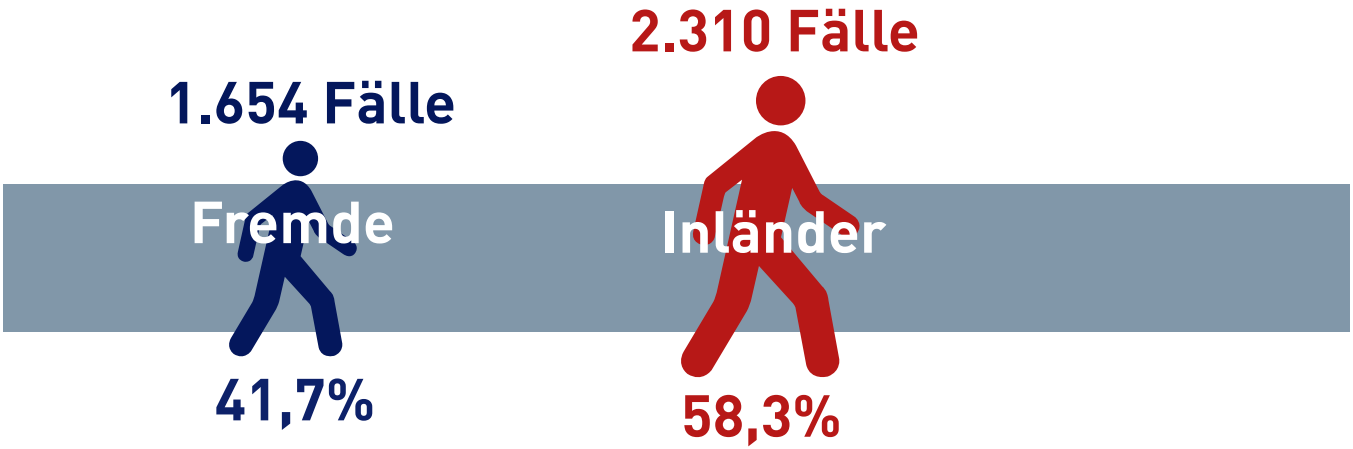


Die Anzahl angezeigter Fälle nach § 126b StGB (Störung der Funktionsfähigkeit eines Computersystems) stieg von elf (2004) auf 470 (2013), was einer Steigerungsrate von über 4.000 Prozent entspricht. An diesen fortgesetzt hohen Steigerungsraten über die letzten zehn Jahre kann abgelesen werden, dass mit der zunehmenden Verbreitung von Computern, dem Ausbau von Netzwerken und Breitbandverbindungen im vergangenen Jahrzehnt das Deliktsfeld Cybercrime einen enormen Anstieg zu verzeichnen hatte. Gleichzeitig sind aufgrund des Vorhandenseins massenhafter Technologien der Informations- und Kommunikationstechnik (IKT) neue Kriminalitätsphänomene entstanden, wobei weiterhin von einem großen Dunkelfeld im Bereich Cybercrime auszugehen ist.

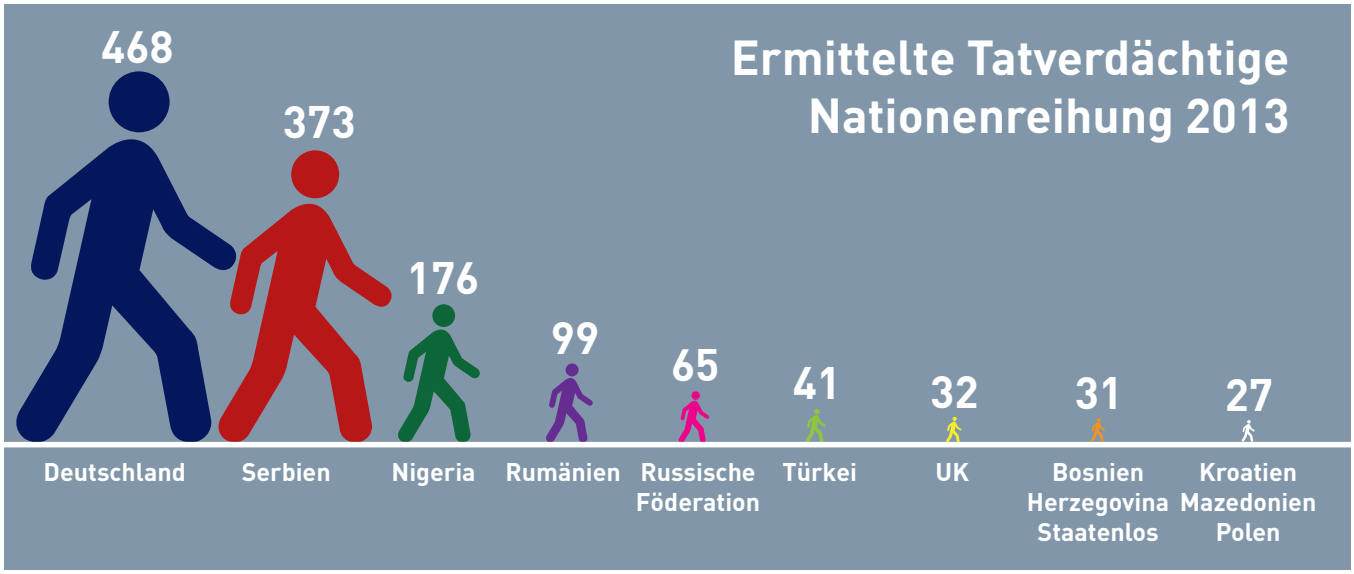
Bei den Tatverdächtigen ist mit rund 46 Prozent die stärkste Gruppe die der 25- bis 40-Jährigen (2012: ebenfalls 46 Prozent), gefolgt von den über 40-Jährigen mit rund 27 Prozent (2012: 28 Prozent).



Im Jahr 2013 stammten von den ermittelten Tätern rund 58 Prozent aus dem Inland.



Der Anteil an Nicht-Österreicherinnen und Nicht-Österreichern beträgt 42 Prozent, wobei Deutschland mit sieben Prozent und Türkei mit drei Prozent den größten Anteil stellen. Hier wirkt sich die räumliche und sprachliche Nähe zu Deutschland aus, vor allem bei Betrugsfällen im Internet. Ansonsten ist schwerpunktmäßig eine Verteilung der Täter in Osteuropa zu erkennen.



Die Tricks der Computerkriminellen

Vermeintliche Gratis-Angebote, Phishing-E-Mails, gefälschte Gewinnbenachrichtigungen, Love Scam usw. – die Bandbreite beim Internetbetrug ist groß. Und das Internet bietet den Tätern Anonymisierungsmöglichkeiten, eine größere Reichweite und eine schnelle Vorgehensweise unter Nutzung ständig wechselnder falscher Identitäten. Vielfach agieren die Täter aus dem Ausland und verschleiern ihre Spuren, wodurch eine Nachverfolgung für die Strafverfolgungsbehörden in Österreich deutlich erschwert wird. Um forensische Spuren sicherzustellen, ist eine rasche Reaktion der Polizei notwendig. Die zuverlässige internationale Kooperation ist entscheidend, um Täter ausforschen zu können.

Typischerweise werden beim Internetbetrug die neuen Medien zur Kontaktherstellung mit potenziellen Opfern benutzt. Das Ziel der Täter ist die Erwirkung einer Geldleistung von den Opfern. Der teilweise sorglose Umgang der Bevölkerung bei der Nutzung des Internets und der neuen Medien vereinfacht den Tätern die Begehung der Straftaten. Internetuser finden sich – im Gegensatz zur realen Welt – auch damit ab, Opfer eines Betrugs werden zu können. Geschädigte Firmen erstatten oft keine Anzeigen, um ihre Reputation zu wahren.

Gängige Betrugsarten:

Phishing

Hier arbeiten mehrere Täter in verschiedenen Teilbereichen organisiert zusammen. Die Kontaktaufnahme zwischen Täter und Opfer erfolgt meist durch Spam-E-Mail. Diese erwecken den Anschein eines offiziellen E-Mails von österreichischen Bankinstituten, das Layout ist zumeist sehr gut nachgeahmt. Die Opfer werden angehalten, Zugangsdaten zu deren Bank-Accounts und persönliche Kontaktdaten, wie zum Beispiel Telefonnummern bekanntzugeben. Dazu sollen die Opfer einem Link im Spam-E-Mail folgen. Dieser Link öffnet ein Onlineformular zur Dateneingabe, das zumeist auf einem von den Tätern kontrollierten Server liegt. Den Opfern wird avisiert, dass nach Eingabe dieser Daten eine telefonische Kontaktaufnahme durch die Sicherheitsabteilung der Bank erfolgen wird. Nach Eingabe der Daten in das Formular erfolgt der Einstieg in den Netbanking-Account des Opfers durch den Täter. Gleichzeitig erfolgt ein telefonischer Kontakt zum Opfer. Hier wird dem Opfer mit dem Hinweis, die Sicherheit des Accounts zu überprüfen, oder ein Sicherheitsfeature aktivieren zu müssen, ein TAN oder TAC herausgelockt. Der TAN/TAC wird entweder für die Generierung einer Überweisung oder zur Umstellung des Authentifizierungsverfahrens genutzt. Die neuen Codes bestellt der Täter auf eine für ihn zugängliche Adresse. Der Vorteil dieser Methode ist, dass der Täter somit mehrere TAN/TAC zur Verfügung hat und so auch mehrere Überweisungen – und damit zumeist einen höheren Gesamtbetrag – generieren kann, ohne dem Opfer dafür immer wieder einen neuen Transaktionscode entlocken zu müssen. Das Geld wird auf Konten von Finanzagenten überwiesen und in weiterer Folge via Geldtransferdienste weitergeleitet.

Hacking

Unter Hacking versteht man die Schaffung eines unberechtigten Zugangs zu Computersystemen unter Überwindung der Sicherheitssysteme. Ziel der Hacker ist die Überwindung der Sicherheitsmechanismen, um Schwachstellen aufzudecken oder für ihre Zwecke auszunützen. Vorwiegende Motive sind Betrugsabsicht, Langeweile, Geltungsdrang oder Nachahmung an.

EUROPOL-Operation „BlackShades“

Im Sommer 2013 begann man im Cybercrime-Competence-Center im Bundeskriminalamt (C4) aufgrund eines Hinweises vom Federal Bureau of Investigation (FBI) in Österreich mit Ermittlungen gegen international agierende Hacker. Dabei konnten in Österreich 19 Tatverdächtige ausgeforscht und eine Datenmenge in der Höhe von 56 Terrabyte sichergestellt werden. Weltweit wurden 97 Personen festgenommen. Die Hacker verwendeten eine Schadsoftware, mit der fremde Computersysteme übernommen wurden. So konnten strafbare Handlungen, wie Phishing-Attacken, Accounthacking und -diebstahl, Denial-of-Service-Attacken, Verbreitung von Spammails und Computerviren als auch der Aufbau von BotNetzwerken verübt werden.

Betrügerischer Datenverarbeitungsmissbrauch

Organisiert operierende Täter arbeiten in diesem Deliktsbereich eng zusammen. Im ersten Schritt werden Computer mit einem Minimalprogramm infiziert, das den Tätern erlaubt, über einen Command & Control-Server die Kontrolle über diese Computer zu übernehmen. Die Infektion erfolgt entweder mittels Spam-E-Mail (Anlagen mit eingebettetem Schadprogramm), oder durch Drive-by-Download. Hier werden gezielt Sicherheitslücken im Browser beim Besuchen einer Webseite ausgenützt. Anschließend wird das eigentliche Schadprogramm während des laufenden Geschäftsvorgangs unbemerkt auf den Computer des Opfers geladen und eine gefälschte Überweisung generiert. Dem Opfer wird der TAN zwecks angeblich zu installierende Sicherheitsfeatures oder Demoüberweisungen herausgelockt. Bei dieser Deliktsart gibt es zahlreiche Varianten. Des Weiteren werden Mobiltelefone der Opfer mit Schadprogrammen infiziert, um das TAC-/mTAN-System zu umgehen. Die Beträge werden auf Konten von Finanzagenten überwiesen und in weiterer Folge via Money-Transmitter weitergeleitet.

Bestellbetrug

Beim Bestellbetrug gibt es zwei Vorgehensweisen: Einerseits werden Waren mit dem Vorsatz bestellt, diese nicht zu bezahlen. Dabei werden falsche Namen angegeben oder die versandten Pakete mit einer falschen Unterschrift angenommen. Da der Betrüger unter einer falschen Identität auftritt, kann die Forderung zumeist nicht eingetrieben werden. Andererseits bieten Täter Waren jeglicher Art zum Kauf an. Die „Jagd nach Schnäppchen“ der Internetuser räumt den Tätern immer mehr Möglichkeiten ein, Waren oder Dienstleistungen

zu Betrugszwecken anzubieten. Die Käuferinnen und Käufer bezahlen die Kaufsumme, erhalten jedoch die Waren nicht, da diese nie vorhanden waren bzw. nicht die Absicht bestand, diese zu versenden.

Missbräuchliche Verwendung von Kreditkartendaten im Internet

Betrügerisch erlangte Kreditkartendaten werden im Internet zur Bezahlung von Waren, Buchung von Flügen und Dienstleistungen verwendet. Der Situation Report von Europol geht von einem jährlichen Profit von 900 Millionen Euro durch missbräuchliche Verwendung von Kreditkartendaten im Internet in Europa aus.

Inkassobetrug

Immer wieder erhalten Unternehmen sowie Bürgerinnen und Bürger E-Mails, in denen sie aufgefordert werden, einen angeblich offenen Rechnungsbetrag einzuzahlen – oft in Zusammenhang mit einem angeblichen Eintrag in ein Register.

Gewinnversprechen

Das Versprechen angeblich hoher Gewinne ist eine Masche, die Betrüger in unterschiedlichen Varianten anwenden. Vor einer möglichen Inanspruchnahme des angeblichen Gewinns werden aber Vorauszahlungen für die Freigabe des Gewinns und für andere Zahlungen verlangt. Der vorgetäuschte Gewinn wird nie ausbezahlt.

Notfall-Emails

Die Täter erlangen durch Hacking- oder Phishing-Attacken die Zugangsdaten von E-Mail-Accounts bei Freemail-Anbietern und übernehmen diese Konten. Sie nutzen die in den Postfächern vorhandenen oder im Adressbuch gespeicherten Kontakte, schreiben diese Personen an und täuschen den Empfängern der E-Mails vor, dass dem Inhaber des Accounts ein Notfall im Ausland widerfahren ist. Die Empfänger werden aufgefordert, einen bestimmten Betrag als Unterstützung zu überweisen – meist über einen Zahlungsdienstleister.

„Lovescam“ oder „Datingscam“

Beim „Love Scam“ versuchen die Betrüger durch das Vortäuschen einer fiktiven Liebesbeziehung vom Opfer Geld zu erhalten. Die Täter nehmen unter anderem über Singlebörsen und Social Networks Kontakt mit den Opfern auf. Nach einiger Zeit wird unter Vortäuschung falscher Tatsachen um Geld gebeten. So benötigen die Täter beispielsweise Geld für die Reise zu einem gemeinsamen Treffen, für die Heilungskosten für sich selbst oder eines nahen Angehörigen oder für Ausgaben, um den Kontakt aufrechterhalten zu können.

Finanzagenten („Money Mules“)

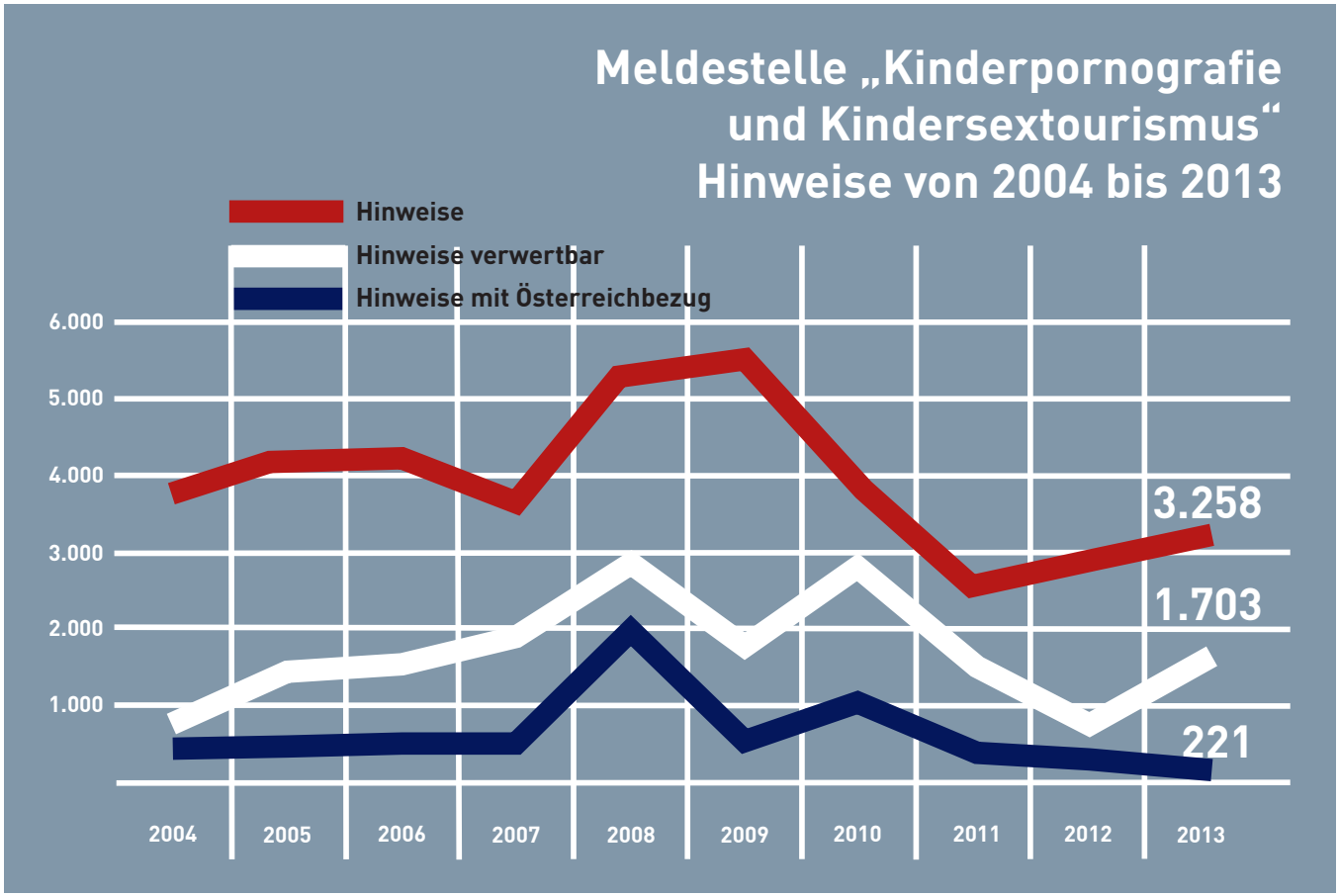
Geldwäscher versuchen ahnungslose Bürgerinnen und Bürger über Stellenanzeigen als „Finanzagenten“ („Money Mules“) anzuwerben. Oftmals wird diese Tätigkeit als Nebenjob angeboten. (Betreff: „Arbeit für dich“). Gegen Provision sollen die Angeworbenen dann ihr Konto für Geldtransfers zur Verfügung stellen, das heißt, Zahlungen entgegennehmen und an unbekannte Dritte weiterleiten. Das Problem dabei: Wer bei einem solchen Geldwäschetransfer mitmacht, macht sich strafbar. Der Finanzagent dient lediglich dazu, die Spur des Geldes für die Nachverfolgung durch die Strafverfolgungsbehörden intransparent zu machen und die illegal erlangten Gelder möglichst schnell und über mehrere Stationen ins Zielland zu transferieren. Beteiligt man sich als Finanzagent an diesem Geldtransfer, so kann man sich einer Mittäterschaft zur Geldwäscherei oder des Betrugs strafbar machen.

Angriffe auf Social Media-Accounts

Soziale Netzwerke wie Facebook, Twitter usw. werden vor allem durch Malware, Hacker und Personen aus dem Lebensumfeld angegriffen. Ungeeignete Passwörter, zu viel Vertrauen, ein sorgloser Umgang mit Informationen und ein unbeschränkter Zugang zu den Profilen sind wichtige Parameter, die bei Attacken auf soziale Netzwerke hilfreich sind. Nach Erlangen der Login-Informationen wird in vielen Fällen die Identität missbraucht, um befreundeten und bekannten Personen beispielsweise eine Notlage vorzutäuschen und somit Geldüberweisungen zu veranlassen. Die Täter löschen nach dem E-Mailversand alle Kontakte und vergeben ein neues Passwort, damit der eigentliche Besitzer nicht mehr einsteigen kann. Häufig verschaffen sich Täter auch den Zugang zu Social-Media-Accounts, um Nutzerprofile zu ändern bzw. die Besitzerin oder den Besitzer des Profils in einem schlechten Licht erscheinen zu lassen. Meist werden solche Taten von Personen aus dem Lebensumfeld der Geschädigten oder des Geschädigten verübt. Motive sind dabei oft Rache, Neid oder Eifersucht. Auch im unternehmerischen Umfeld spielt der klassische Identitätsdiebstahl eine wichtige Rolle, um beispielsweise an Firmeninformationen zu gelangen.

Kinderpornografie

Kinderpornografie ist in § 207a StGB (Pornografische Darstellungen Minderjähriger) geregelt. Der Straftatbestand betrifft die die Herstellung, Verbreitung und den Besitz von pornografischen Darstellungen von Kindern und Jugendlichen. Mit 1. Jänner 2012 wurde der neue § 208a StGB („Anbahnung von Sexualkontakten zu Unmündigen") eingeführt, womit es nunmehr auch einen Straftatbestand für Cybergrooming im österreichischen Strafrecht gibt. Im Jahr 2013 wurden in der Meldestelle „Kinderpornografie und Kindersextourismus" 3.258 Hinweise bearbeitet, davon haben 221 Hinweise einen Österreichbezug.



2013 wurden in Österreich 551 Anzeigen nach § 207a StGB erstattet; 2012 waren es 572 Anzeigen.

Professionalisierung in der Bekämpfung von Cyber-Kriminalität

Um diesen Trends wirkungsvoll begegnen zu können, waren die Umsetzung der Cybersicherheitsstrategie und die Implementierung des Cybercrime-Competence-Centers (C4) im Bundeskriminalamt notwendige und richtige Weichenstellungen. Das Jahr 2013 stand daher ganz im Zeichen der Professionalisierung und unter einer Ausbildungsoffensive:

- **Grundausbildung:** Die Polizistinnen und Polizisten auf der Ebene der Polizeiinspektionen, der Stadtpolizeikommanden und der Bezirkspolizeikommanden erhalten in der Grundausbildung sowie im Zuge ihrer Laufbahnausbildung zu dienstführenden Beamten sowie bei Fortbildungsmaßnahmen Basisschulungen zum Thema IT-Kriminalität.
- **Spezialschulungen:** Neben den auch 2013 fortgesetzten Spezialschulungen für die operativ tätigen Kriminalbeamtinnen und -beamten wurden neuerlich sieben Bezirks-IT-Ermittler-Kurse durchgeführt, wodurch 105 Bezirks-IT-Ermittlerinnen und -Ermittler für den Dienst auf Ebene der Polizeiinspektionen ausgebildet werden konnten. Die Aufgabe dieser Beamtinnen und Beamten besteht einerseits in der Unterstützung bei der IT-Beweissicherung. Andererseits bilden sie die Schnittstelle zwischen der täglichen Polizeiarbeit an der Basis und den Bereichen IT-Forensik und Cybercrime-Ermittlungen in den Landeskriminalämtern. Derzeit befinden sich österreichweit 182 Bezirks-IT-Ermittlerinnen und -Ermittler zur Unterstützung des Assistenzbereichs IT-Beweismittelsicherung und Cybercrime-Ermittlungen im Einsatz.
- **Kooperationen:** Die enge und gute Kooperation des C4 mit dem Bundesministerium für Justiz (BMJ) spiegelt sich unter anderem auch im Bereich gegenseitiger Aus- und Fortbildungsmaßnahmen wider. So hielten Experten des C4 spezielle Schulungen für Richterinnen und Richter sowie Staatsanwältinnen und Staatsanwälte unter anderem am Oberlandesgericht in Linz ab.
- **Nationalen und internationale Schulungsveranstaltungen:** Die Cybercrime-Ermittlerinnen und -Ermittler sowie IT-Forensikerinnen und -Forensiker in den Landeskriminalämtern und im C4 nahmen an nationalen und internationalen Schulungen und Spezialtrainings teil, etwa an Veranstaltungen der „International Association for Computer Informations Systems“ (IACIS) und der „European Cybercrime Training and Education Group“ (ECTEG).

Das Kompetenzzentrum C⁴

Clickjacking, Denial of Service, Fake Donation Sites, Exploit Kits, Key Loggers, Malicious Links, Phishing, Social Engineering, Rouge Certificates, Spam, Ransomware, Spear Phishing, Spoofing, Viren, Trojaner, Würmer, Scam, Spam, Hacktivism, Social Media Crime, Drive by Exploits, Bot-Nets, Code Injection, Scareware, Identity Theft, Illicit Goods Trading, Financial Online Fraud. Diese beispielhafte Auflistung dokumentiert, wie zahlreich und vielfältig die Bedrohungen im Cyberspace geworden sind. Diese Bedrohungen sind die gängigsten und betreffen die Wirtschaft, deren Kunden und Beschäftige, Behörden, Ärztinnen und Ärzte, Patientinnen und Patienten und jede private Nutzerin und Nutzer. Sie bewirken finanzielle Schäden, Reputationsverlust und können sogar eine Gefahr für Leib und Leben bedeuten. Als Antwort auf diese Bedrohungen wurde auf Grundlage der Cybercrime-Strategie des BMI das C⁴ im Bundeskriminalamt mit Beginn 2012 etabliert. Cybercrime als Querschnittsmaterie erfordert einen breiten Ansatz zu ihrer Bekämpfung. So ist es Aufgabe des C⁴, unter anderem die Schnittstelle zum „European Cybercrime Centre" (EC3) bei Europol und zum „Digital Crime Center" (IDCC) bei Interpol zu bilden sowie bestehende Kooperationen mit Wirtschaft und Forschung auszubauen, um für den notwendigen Wissens- und Informationstransfer zu sorgen.

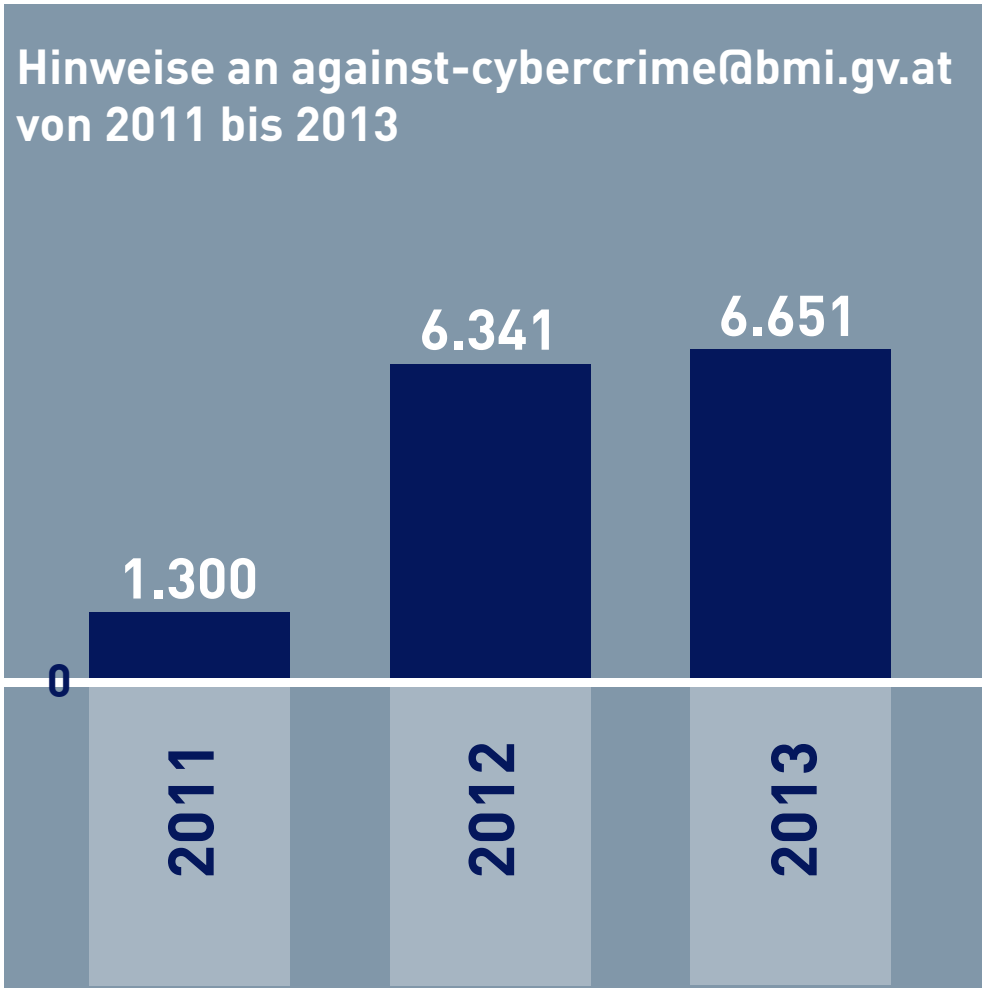
Das C⁴ realisiert die zentrale Funktion einer nationalen Schnitt- und Meldestelle sowohl innerhalb der polizeilichen Organisation als auch für Bürgerinnen und Bürger.

Das C⁴ fokussiert auf Cybercrime-Delikte im engeren Sinn, die sich auf die Vertraulichkeit, die Integrität und die Verfügbarkeit von Daten in Netzwerken und den darin eingebundenen Geräten beziehen. Informationstechnologie (IT) ist hier nicht nur Tatwerkzeug, sondern auch Angriffsziel selbst. Im Gegensatz dazu ist bei Cybercrime im weiteren Sinn die IT nur ein Tatwerkzeug, um eine „klassische" kriminelle Handlung zu planen oder zu begehen. In diesen Fällen unterstützt das C⁴ die originär zuständigen Abteilungen des BK und der Landeskriminalämter sowie andere Behörden und Ministerien mit forensischer Sicherung, Auswertung und Analyse digitaler Spuren als auch mit fachspezifischen Ermittlungen.

Ein weiterer Schwerpunkt des C⁴ ist die Sensibilisierung und Ausbildung im Bereich Cybercrime sowie Informationen über den sicheren Umgang mit Informationstechnologien. Dies steht im Einklang mit der „Österreichischen Strategie für Cyber Sicherheit" (ÖSCS) und soll für die nötige Sensibilisierung aller Zielgruppen sorgen, um so durch Bewusstseinsbildung das Verständnis für Cyber-Sicherheit zu schaffen. Zielgerichtet und fachlich kompetent soll so die Anfälligkeit für Cybercrime-Delikte gemindert und eine Erhöhung der Resilienz erreicht werden.

Ansprechstelle für Betroffene

Im Mai 2011 wurde die Meldestelle against-cybercrime@bmi.gv.at eingerichtet. Bürgerinnen und Bürger können rund um die Uhr verdächtige Wahrnehmungen im Internet melden. Im Jahr 2013 gab es eine leichte Steigerung auf 6.651 E-Mails. Nach wie vor betreffen die Meldungen vor allem Internetbetrugsfälle mit eher geringen Schadenssummen sowie Massenmails, die an private Postfächer gesendet werden und mit hohen Gewinnen locken („419er-Briefe", Lotteriegewinne etc.). Ebenfalls gestiegen ist die Zahl der Meldungen über Phishing-Versuche, den „Polizeitrojaner" und „Notfall"-E-Mails.



Beweissicherung und Analyse

Um Daten erfolgreich auswerten zu können, werden international anerkannte, erfolgreiche Methoden eingesetzt. Standardmäßig stehen ihnen dafür auch spezielle Hardwareausstattungen sowie verschiedene forensische Hard- und Softwareprodukte zur Verfügung. Die immer häufigere Verwendung von mobilen IT-Geräten wie Smartphones und Tablets stellt auch die Sicherheits- und Strafverfolgungsbehörden vor immer neue Herausforderungen. Die Möglichkeit, Daten in der „Cloud" zu speichern, wird immer beliebter, was die Ermittlungsarbeit insbesondere auch im Bereich der IT-Forensik zusätzlich erschwert.

Im Spezialgebiet Datensicherung zeigt sich ein eindeutiger Trend zu mobilen Geräten. Hier gab es 2013 einen Anstieg von über 50 Prozent gegenüber dem Jahr davor.

Für eine erfolgreiche Beweissicherung, -aufbereitung und -auswertung der auf dem Speichermedium sichergestellten Daten ist spezielles Fachwissen und viel praktische Erfahrung notwendig. Dieses Know-how im Bereich der IT-Forensik wird durch die regelmäßige Teilnahme an entsprechenden Spezialtrainings im In- und Ausland sichergestellt.

Hand in Hand mit Wissenschaft und Wirtschaft

Eine enge nationale und internationale Zusammenarbeit der Sicherheitsbehörden mit Spezialistinnen und Spezialisten aus Wirtschaft, Forschung, Wissenschaft und Telekommunikationsunternehmen ist ein wesentlicher Bestandteil für die effektive Bekämpfung der IT-Kriminalität. In den letzten Jahren wurden dafür mehrere Projekte und Kooperationen umgesetzt, die jetzt intensiviert und ausgebaut wurden. Wie in den Jahren zuvor wurden auch 2013 Initiativen erfolgreich gestartet bzw. umgesetzt:

- **Projekt „IT-Sicherheit“:** Dieses Projekt läuft seit mehreren Jahren und soll einen rascheren Informationsausaustausch zwischen dem BMI und der Wirtschaftskammer Österreich (WKO) erzielen. Wirksame Maßnahmen zur IT- und Datensicherheit für heimische Unternehmen werden immer wichtiger, da das Gefahrenpotenzial von Cyberattacken ständig zunimmt. Dazu wurden ein Informationsfolder erstellt und eine Internetplattform sowie IT-Sicherheitshandbücher von der WKO zur Verfügung gestellt. Auf der Internetplattform „IT-Safe“ werden Warnmeldungen des Bundeskriminalamts eingestellt, um so die Information möglichst rasch und zielgerichtet an die Unternehmen weiterzugeben. Mehr Informationen finden Sie unter www.it-safe.at
- **Kooperation mit Hochschulen und universitären Einrichtungen:** Die Zusammenarbeit mit Hochschulen und universitären Einrichtungen ist generell von großem Interesse, da sie dazu beiträgt, grundlegendes Wissen und Know-how für die polizeiliche Arbeit zu schaffen. So wird derzeit ein neues Ausbildungskonzept erarbeitet, dessen Schwerpunkt in der Praxisorientierung liegt. Neben regelmäßigen Weiterbildungsveranstaltungen in Bezug auf neue IT-Entwicklungen werden die IT-Forensikerinnen und -Forensiker des Bundeskriminalamts auch zu internationalen Schulungsaktivitäten entsandt, etwa bei der ECTEG. In dieser bei Europol angesiedelten Arbeitsgruppe werden auf europäischer Ebene Trainingsprogramme für IT-Forensik und IT-Ermittlungen erstellt und weiterentwickelt.
- **KIRAS - Das Österreichische Förderungsprogramm für Sicherheitsforschung:** Auch 2013 wurden wieder Projekte eingereicht oder abgeschlossen, etwa die Projekte „Social Media Crime“ und „SMD4Austria. Social-Media-Dienste für Sicherheit und Prävention in Österreich“.
- **Symposium „Neue Technologien“ – Internationale Konferenz zum Austausch von Informationen über Technologien der Zukunft mit Auswirkungen auf die polizeiliche Arbeit:** Auch 2013 fand das Symposium „Neue Technologien“ in Bern/Schweiz statt. Die vom österreichischen Bundeskriminalamt, dem Schweizer Bundesamt für Polizei (FedPol), dem Landeskriminalamt Bayern und dem deutschen Bundeskriminalamt organisierte Konferenz zeigte einmal mehr, welche Technologien in absehbarer Zeit das Spektrum der polizeilichen Arbeit beeinflussen werden. Hochkarätige Vortragende aus Wirtschaft, Wissenschaft und Forschung informierten das internationale Publikum über Themen mit dem Motto „Ubiquitäres Computing. Abschied von der analogen Welt“. Ziel der Konferenz war es, mit einem Technologieausblick die polizeiliche Arbeit im Hinblick auf diese neuen Technologien zu beleuchten und die damit verbundenen Chancen und Risiken einzuschätzen.

Internationale Zusammenarbeit

Ein Charakteristikum des Internets ist, dass es keine Landesgrenzen kennt und damit in Sekundenbruchteilen Informationen zwischen verschiedenen Rechtssystemen verschoben werden können, womit auch rechtliche Schwierigkeiten bei der Bekämpfung von Cybercrime verbunden sind. Keine andere Kriminalitätsform ist derart schnelllebig und in ihrer Bekämpfung so abhängig von internationaler Kooperation wie Cybercrime.

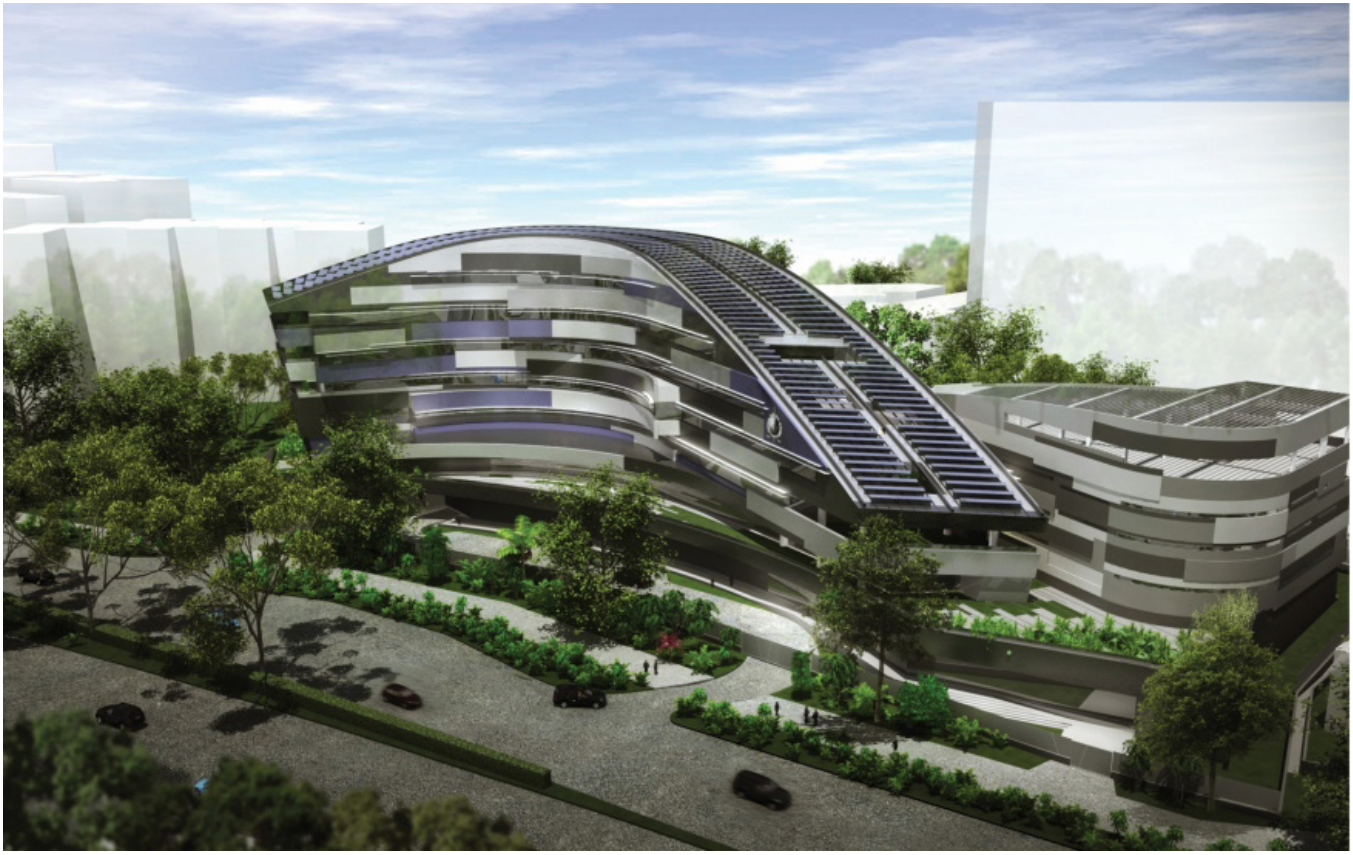
Zudem dringt Cybercrime in immer weitere Bereiche der Gesellschaft vor; immer mehr Menschen sind via Internet mit der Welt verbunden. Dieser Umstand ermöglicht es auch kriminellen Gruppierungen leichter, an potenzielle Opfer heranzukommen. Mangelndes technisches Verständnis der User und deren unvorsichtiger Umgang mit persönlichen Informationen im Internet erleichtern es Kriminellen, Straftaten zu begehen.

Die Reaktion darauf ist eine verstärkte Zusammenarbeit im Bereich der Cybercrime-Bekämpfung. So wurde im Jänner 2013 das European Cybercrime Center (EC3) bei Europol eingerichtet, um die Strafverfolgung im Bereich Cybercrime zu stärken und die Bürgerinnen und Bürger sowie die Wirtschaft besser zu schützen. Die Schaffung des EC3 war eine Priorität der EU-Sicherheitsstrategie.

Das EC3 wurde insbesondere eingerichtet, um in folgenden drei Bereichen signifikante Unterstützung für die Mitgliedsstaaten zu schaffen:

- Bekämpfung von Cybercrime, begangen durch organisierte Gruppierungen, die beispielsweise durch Online-Betrug große Geldmengen erbeuten.
- Bekämpfung von Cybercrime-Formen, die die Opfer massiv schädigt, wie beispielsweise sexueller Missbrauch von Kindern.
- Bekämpfung von Cybercrime (inklusive Cyber Attacks), gerichtet gegen kritische Infrastruktur und Informationssysteme der EU-Mitgliedstaaten.

Infrastruktur und Informationssysteme der EU-Mitgliedstaaten.
Im Rahmen des EU-Policy-Cycle 2014 bis 2017 gegen schwere und organisierte internationale Kriminalität ist Cybercrime eine von neun Prioritäten des Rates, wobei das EC3 einen wesentlichen Teil bei der Umsetzung dieser Priorität beisteuert. Österreich beteiligt sich aktiv in allen drei Sub-Prioritäten.



Interpol errichtet derzeit den „Interpol Global Complex for Innovation“ (IGCI) in Singapur. Das IGCI soll Top-Forschungs- und Entwicklungseinrichtung zur Identifikation von Cyberdelikten und Kriminellen sein, innovatives Training kreieren und operativen Support für die Interpolstaaten bieten. Die drei wichtigsten Komponenten des IGCI sind

- digitale Sicherheit
- Kapazitätsaufbau und Training
- operativer und investigativer Support

Das EC3 und der IGCI arbeiten eng zusammen und unterstützen sich gegenseitig. Einmal jährlich findet eine Interpol-Europol-Cybercrime-Konferenz statt, an der auch Personen aus dem privaten Sektor teilnehmen, um die Herausforderungen im Bereich Cybercrime gemeinsam zu erörtern. 2013 fand die Konferenz bei Europol in Den Haag statt, 2014 wird sie in Singapur abgehalten.

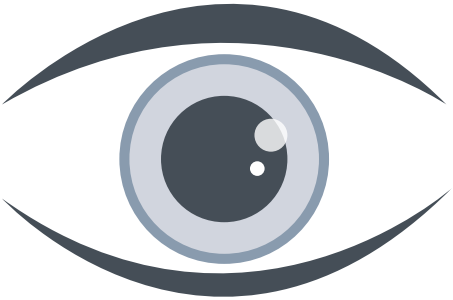
Jugendpräventionsprojekte

Kinder und Jugendliche sind oft unbekümmert und neugierig, benötigen Aufmerksamkeit und Anerkennung, wünschen Freiheit, suchen Orientierung und versuchen, ihre Identität auszubilden. Das Internet spielt dabei eine wesentliche Rolle. Dabei können sie zum Täter, aber auch zum Opfer werden. Die Erwachsenen unterschätzen oft die Risiken. Information und Prävention sind wichtige Maßnahmen, um Kinder zu problem- und verantwortungsbewussten Erwachsenen zu machen.

Das Projekt „Click & Check“ wird österreichweit sehr erfolgreich umgesetzt. Dabei informieren eigens geschulte Polizistinnen und Polizisten Jugendliche in den Schulen über „Happy Slapping“ und „Cyberbullying“ oder „Cybermobbying“ und versuchen anhand kurzer Videofilme, das Unrechtsbewusstsein von Jugendlichen zu fördern und Gesetzesinformationen zu vermitteln. Im Jahr 2013 wurden österreichweit 38.514 Kinder und Jugendliche über den richtigen, sicheren Umgang mit Handy und PC informiert und sensibilisiert.

2013 standen die Gefahren von „Cybergrooming“ im Projekt „Jugend OK“ im Vordergrund. In den Aktionsmonaten von Oktober bis Dezember wurden Jugendliche mittels Aktionskarten auf die Gefahren aufmerksam gemacht. In diesem Zeitraum wurden weitere 32.302 Jugendliche über die Gefahren im Internet informiert.

Ausblick



Die immer weiter voranschreitende Vernetzung und die damit einhergehende Verfügbarkeit von schnellen Breitbanddatenverbindungen ist nicht nur für die legale Wirtschaft ein wesentlicher Vorteil, sondern bietet auch für Cyberkriminelle die Grundlage zur effizienten Entwicklung und Vermarktung ihrer illegalen Geschäftsmodelle. „Cybercrime as a Service", also das Zukaufen oder Anmieten von kriminellen, digitalen Dienstleistungen wie z.B. Schadprogrammen, Hacking-Tools, Botnetzen usw. auf den Plattformen der „Underground Economy" ermöglicht es beinahe jedem, sich dieser Methoden für kriminelle Zwecke zu bedienen.

Speziell durch den Einzug neuer digitaler Technologien in unser tägliches Leben wird die Entstehung neuer Erscheinungsformen von Cyberkriminalität begünstigt. Als Beispiel kann hier der Einsatz von „NFC" (Near Field Communication) zur Durchführung kontaktloser Zahlungsvorgänge angeführt werden, mit welcher Zahlungen zum Teil ohne PIN-Eingabe möglich sind. Aber auch Verkehrsmittel werden mit der Möglichkeit zur Netzwerk-Kommunikation ausgestattet wie zum Beispiel Smart-Vehicles und Drohnen, welche in naher Zukunft vermehrt im Straßen- und Luftverkehr zum Einsatz kommen werden. Durch das „Internet of things", bei dem technische Geräte vernetzt kommunizieren wie zum Beispiel Kühlschranke, Smart-TVs aber auch medizinische Apparate, wird unser Leben nicht nur optimiert, sondern auch anfälliger für Angriffe jeglicher Art in diesem Bereich.

Die intensive Nutzung von Sozialen Medien, allen voran Facebook und Twitter, sowie neue Trends wie zum Beispiel „Google-Glass" oder der Einsatz von „action cams", machen immer mehr individuelle Lebensbereiche öffentlich sichtbar und damit auch für Kriminelle transparent.

Die Folge davon ist eine vermehrte direkte Kontaktaufnahme von Cyberkriminellen mit ihren potentiellen Opfern, sowie eine aggressivere Vorgangsweise bei der Tatbegehung bis hin zur Erpressung durch direkte Drohung mit Gewalt.

Diesen Herausforderungen kann nur durch die Beschreitung neuer Wege in der internationalen Zusammenarbeit sowie der engen Kooperation von Wirtschaft und Forschung mit den zuständigen Behörden begegnet werden. Von besonderer Bedeutung dabei ist, der noch immer weit verbreiteten Sorglosigkeit der „Userinnern und User" bei der Nutzung des Internets durch Prävention gezielt entgegen zu wirken. Ein spezielles Augenmerk ist dabei dem Bereich der Kinder und Jugendlichen zu schenken, welche mit diesen Medien immer früher in Kontakt kommen sowie Senioren einen sicheren Einstieg und Umgang mit dieser Materie zu ermöglichen.

Glossar:

Antivirenprogramm (auch Virenscanner oder Virenschutz genannt): iSoftware, die bekannte Computerviren, Computerwürmer und Trojanische Pferde aufspürt, blockiert und gegebenenfalls beseitigt. Die Mehrzahl dieser Programme identifiziert Schadcode anhand von Signaturen, ohne die Schadsoftware oft unerkannt bleiben kann.

Backdoor: Schadfunktion, die üblicherweise durch Viren, Würmer oder Trojanische Pferde eingebracht und installiert wird. Es ermöglicht Dritten einen unbefugten Zugang („Hintertür") zum Computer, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen. Backdoors werden oft genutzt, um den kompromittierten Computer als Spamverteiler oder für Denial-of-Service-Angriffe zu missbrauchen.

BotNet (Bot-Netz): (Kurzform von „Roboter Netzwerk");fernsteuerbares Netzwerk im Internet von Computersystemen, das aus untereinander kommunizierenden Bots besteht. Diese Kontrolle wird durch Würmer bzw. Trojanische Pferde erreicht, die den Computer infizieren und dann auf Anweisungen warten. Diese Netzwerke können für Spam-Verbreitung, (Distributed-)Denial-of-Service-Attacken usw. verwendet werden, zum Teil, ohne dass die betroffenen Computersystem-Benutzer etwas davon bemerken. Zur Steuerung dieser Roboterarmee im Netzwerk werden sogenannte Command & Control-Server (C&C-Server) eingesetzt.

Bot: Überbegriff für ein Programm, das vorwiegend verwendet wird, um Aufgaben automatisiert durchzuführen. In der Regel auch als übernommener Rechner bezeichnet, der in ein BotNet eingebunden wurde.

Browser: Webbrowser (engl. für „Durchstöberer", „Blätterer") sind spezielle Computerprogramme zum Betrachten von Seiten im World Wide Web.

Cloud Computing: Speichern von oder Zugriff auf Daten und Anwendungen (Programme) über das Internet anstelle der Nutzung von lokalen Ressourcen wie Festplattenspeicher, Rechenleistung etc. im PC oder in einem lokalen Netzwerk.

Code Injection: iGenerelle Bezeichnung für einen Angriff, bei dem ein Programmcode in eine (Web-)Anwendung (automatisch) eingegeben wird. Dieser Angriff nutzt die schwache Handhabung einer Anwendung aus (Sicherheitseinstellungen, Schwachstellen bei der Programmierung hinsichtlich der Überprüfung von Datenein- und -ausgabe). Bekannt ist die sogenannte SQL-Injektion, bei der in die Datenbankanwendung ein Programmcode eingegeben wird, der bei Abarbeitung im Datenbankprogramm den unberechtigten Zugriff ermöglicht (durch Manipulation der Abfrage-Symantik der Datenbank).

Command & Control-Server (C&C-Server): Zumeist übernommene oder unter falscher Identität angemietete Rechner zur Steuerung der Bots.

Computervirus: Eine nicht selbstständige Programmroutine, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt.

Computerwurm: Ein Computerwurm ähnelt einem Computervirus, verbreitet sich aber direkt über Netzwerke wie dem Internet und versucht, in andere Computer einzudringen. Er verbreitet sich zum Beispiel durch das Versenden infizierter E-Mails (selbstständig durch eine SMTP-Engine oder durch ein E-Mail-Programm), durch IRC-, Peer-to-Peer- und Instant-Messaging-MMS.

Core Cyber Crime: Klassifiziert kriminelle Handlungen gegen das/die Netzwerk(e) selbst, gegen Geräte in diesen Netzwerken oder gegen Dienste und Daten in diesen Netzwerken. Im Wesentlichen dient Cyber-Security dem Schutz der Vertraulichkeit, der Verfügbarkeit und der Integrität der oben angeführten Angriffsziele.

Cybergrooming Anbahnung von Sexualkontakten zu Unmündigen via Internet (z. B. in sozialen Netzwerken etc.).

Darknet: Sammlung von Verfahren und Technologien, die einen anonymen Datenaustausch und Kommunikation im Internet ermöglichen. Es wird auch als „Untergrund-Internet" bezeichnet und wird unter anderem für die Verbreitung von Illegalen Inhalten angewendet.

Deep Web: Bezeichnung für jenen Bereich des Webs, der nur schwer bzw. nicht über Suchmaschinen erreichbar ist. In Verbindung mit Kriminalität können hier auch spezielle Umschlagplätze und geheime Netzwerke („Undernet") gemeint sein. Das Spektrum reicht vom Drogen- und Waffenhandel über Dokumentenfälschung, Geldfälschung, Identitätsdiebstahl und Kinderpornografie bis zu Auftragskiller.

Dialer: Einwahl über Modemverbindungen auf Telefon-Mehrwertrufnummern. Illegale Dialer- Programme führen die Einwahl heimlich durch und fügen dem Opfer finanziellen Schaden zu.

Domain Name System (DNS): Einer der wichtigsten Dienste im Internet. Hauptaufgabe ist die Auflösung des Computernamen oder der URL einer Webseite in eine IP-Adresse.

DoS/DDoS-Attacke: Angriff auf die Verfügbarkeit der Ressourcen und Dienste eines IT-Systems mit dem Ziel, diese zu blockieren und somit regulären Benutzern keinen Zugriff mehr zu ermöglichen. DoS ist die Abkürzung von „Denial of Service" („außer Betrieb setzen"). Bei einer DDoS-Attacke („Distributed Denial of Service") wird der zur Blockade führende Angriff nicht nur von einem Rechner ausgeführt, sondern von mehreren gleichzeitig. Dadurch wird sowohl der Angriff verstärkt als auch die Einleitung von Gegenmaßnahmen erschwert, da diese auf mehrere Quellen angewendet werden müssen.

Drive-by-Download: Unbeabsichtigter/unbemerkter Download von Schadsoftware während des Betrachtens einer Webseite (Drive-by: „im Vorbeifahren"). Realisiert werden Drive-by-Downloads meist über eigens dafür präparierte Webseiten.

Exploit (Zero-Day-Exploit): Ein Exploit (engl. to exploit: ausnutzen) ist eine Software oder eine Sequenz von Befehlen, die spezifische Schwächen bzw. Fehlfunktionen eines anderen Computerprogramms ausnutzen. Ein Exploit, das vor oder am selben Tag erscheint, an dem die Sicherheitslücke (Zero-Day-Lücke) allgemein bekannt

wird, nennt man Zero-Day-Exploit (0-Day-Exploit). Die Gefährlichkeit dieser Exploits rührt daher, dass zu diesem Zeitpunkt kaum ein Hersteller bzw. Entwickler in der Lage ist, die Sicherheitslücke sinnvoll und umfassend mittels eines Patches zu schließen.

Firewall: Netzwerksicherheitskomponente, die Datenverbindungen anhand eines definierten Regelwerks erlaubt oder verbietet. Das Ziel einer Firewall („Brandwand") ist, den Datenverkehr zwischen Netzwerksegmenten mit verschiedenen Vertrauensstufen abzusichern.

IMEI: Die „International Mobile Equipment Identity" (IMEI) ist eine eindeutige 15-stellige Seriennummer, anhand derer jedes GSM- oder UMTS-Endgerät (Mobilstation) eindeutig identifiziert werden kann.

IMSI: Die „International Mobile Subscriber Identity" (IMSI) dient in GSM- und UMTS-Mobilfunknetzen der eindeutigen Identifizierung von Netzteilnehmern (interne Teilnehmerkennung). Neben weiteren Daten wird die IMSI auf einer speziellen Chipkarte, dem „Subscriber Identity Module" (SIM), gespeichert. Die IMSI-Nummer wird weltweit einmalig pro SIM-Karte von den Mobilfunknetzbetreibern vergeben. Die IMSI hat normalerweise nichts mit der Telefonnummer der SIM-Karte zu tun. Die IMSI hat immer 15 Zeichen.

Inhaltsdaten: Inhalte übertragener Nachrichten.

IP-Adresse (Internet-Protocol-Adresse): dEine IP-Adresse dient zur eindeutigen Adressierung von Rechnern und anderen Geräten in einem IP-Netzwerk. Technisch gesehen ist die Nummer eine 32- oder 128-stellige Binärzahl. Das bekannteste Einsatzgebiet für IP-Adressen ist das Internet. Allen am Internet teilnehmenden Rechnern wird eine IP-Adresse zugeteilt. Die IP-Adresse entspricht funktional der Rufnummer in einem Telefonnetz.

Malware: Kurzwort für „Malicious Software" (engl. „malicious": „bösartig"); Computerprogramme, die vom Benutzer unerwünschte bzw. schädliche Funktionen ausführen.

Man In The Middle: Der Angreifer steht entweder physikalisch oder – heute meist – logisch zwischen den beiden Kommunikationspartnern und hat mit seinem System komplette Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmerinnen oder -teilnehmern und kann die Informationen nach Belieben einsehen und sogar manipulieren. Das Besondere des Angreifers besteht darin, dass er den Kommunikationspartnern das jeweilige Gegenüber vortäuschen kann, ohne dass sie es merken.

NFC Near Field Communication (NFC): Nahfeldkommunikation; drahtloser Übertragungsstandard. Neben dem Einsatz als Alternative zum QR-Code hat der NFC-Standard den Vorteil, Informationen in Tags auch beschreiben zu können. So kann über NFC eine Fahrkarte für ein öffentliches Verkehrsmittel erworben werden. Sind diese Informationen im NFC-Chip des Handys gespeichert, so kann selbst bei ausgeschaltetem Handy die Gültigkeit der Fahrkarte geprüft werden. Der elektronische Reisepass verwendet ebenfalls NFC, um Informationen vom Pass bei der Kontrolle auf ein Lesegerät zu übertragen. Neuere Kreditkarten bieten zudem die Möglichkeit, die Bezahlung über NFC abwickeln. Dies könnte NFC auch für Kriminelle attraktiv machen.

Peer to Peer (P2P): In einem Peer-to-Peer-Netz sind alle Computer gleichberechtigt und können sowohl Dienste in Anspruch nehmen als auch Dienste zur Verfügung stellen. Die Computer können als Arbeitsstationen genutzt werden, aber auch Aufgaben im Netz übernehmen.

Phishing: Form des Trickbetrugs im Internet. Dabei wird vor allem per E-Mail versucht, den Empfänger irrezuführen und zur Herausgabe von Zugangsdaten und Passwörtern zu bewegen. Dies bezieht sich in den meisten Fällen auf Online-Banking und andere Bezahlsysteme.

Phreaking: bezeichnet das in der Regel illegale Manipulieren von Telefonsystemen. Dabei ging es normalerweise um die kostenlose Benutzung analoger Telefonleitungen, das Nutzen spezieller kostenfreier Rufnummern für Telefontechniker, über die Verbindungen zu beliebigen Gegenstellen hergestellt werden konnten. „Phreaking" ist ein Kofferwort aus „phone" und „freak".

Polizeitrojaner: siehe Ransomware.

Proxy: (von engl. „proxy representative": Stellvertreter) arbeitet als Vermittler, der auf der einen Seite Anfragen entgegennimmt, um dann über seine eigene IP-Adresse eine Verbindung zur anderen Seite herzustellen. Er übernimmt somit stellvertretend für den anfragenden Clienten die Kommunikation mit dem Ziel oder leitet einfach die Anfragen unter seinem Namen an das Ziel weiter, ohne die Kommunikation selbst zu führen.

QR-Code: Quick-Response-Codes ermöglichen die schnelle Interaktion und Verknüpfung von Offline-Informationen mit Online-Inhalten. In einem Offline-Medium wie einem Werbeplakat, einem Fahrplan an einer Haltestelle oder einer Touristeninformation wird ein QR-Code angebracht. Dieser ermöglicht es dem Benutzer, weiterführende Informationen abzurufen, ohne dazu eine Internetadresse eintippen zu müssen. Da diese QR-Codes meist freizugänglich und somit manipulierbar bzw. überklebbar sind, besteht die Möglichkeit, dass sich Schadsoftware- oder Phishing-Angriffe hinter QR-Codes verstecken können.

Ransomware: Schadsoftware, bei der sich das Opfer durch Überweisung eines Geldbetrags freikaufen kann (engl. „ransom": „feikaufen"). Der Freikauf ist in diesem Zusammenhang mit dem Entfernen einer Sperre oder einer Entschlüsselung von Dateien eines von Ransomware betroffenen Computers zu sehen.

Rogue Certificates: „Gefährliches" Zertifikat. Vertrauenswürdige Zertifikate werden (gegen Bezahlung) von „Certification Authorities" ausgestellt und dienen zur Authentifizierung einer digitalen Identität. Zertifikate werden für eine sichere Kommunikation verwendet. Bei Rogue-Zertifikaten handelt es sich um Zertifikate, die nur den Anschein der Legitimität haben. Je nach Sicherheitseinstellungen im Browser wird unter anderem eine Warnung über ein ungültiges Zertifikat angezeigt, das man annehmen oder abweisen kann.

Scareware: Schadsoftware, die den Empfänger direkt bedroht oder zumindest in Angst versetzen soll. Ein Beispiel ist der „Whats-App-Clown" auf Mobiltelefonen von Kindern.

Server: Software im Rahmen des Client-Server-Konzepts oder eine Hardware (Computer), auf der diese Software (Programm) im Rahmen dieses Konzepts abläuft.

Skriptkiddie: Eine Person, die leicht bedienbare, vorgefertigte Programme benutzt, um unerlaubt in fremde Computer- und Netzwerksysteme einzudringen, oder um durch absichtlich verbreitete Viren, Würmer oder Trojaner Schaden anzurichten.

Social Enginering: Kunst, eine Person zu einer Handlung zu veranlassen oder von etwas zu überzeugen, das objektiv nicht im Interesse dieser Person ist. Oft auch als „the Art of Human Hacking" bezeichnet.

Spam: Unerwünschte, in der Regel auf elektronischem Weg massenhaft übertragene Nachrichten, die dem Empfänger unverlangt zugestellt werden und werbenden Inhalt haben. Dieser Vorgang wird als Spamming oder Spammen bezeichnet, der Verbreiter als Spammer.

Spyware: Programme, die Informationen über die Tätigkeiten des Benutzers sammeln und an Dritte weiterleiten. Ihre Verbreitung erfolgt meist durch Trojaner. Steganografie ist die Wissenschaft der verborgenen Speicherung oder Übermittlung von Informationen in einem Trägermedium.

Transaktionsnummer (TAN): Einmalpasswort, das im Online-Banking verwendet wird. Ein M(obiler)-TAN besteht in der Einbindung des Übertragungskanals SMS. Eine E-TAN ist ein kleines elektronisches Kontrollgerät, dass die (TAN-)Eingabe ersetzt. Während der Kunde bisher eine Liste mit Transaktionsnummern hatte, werden über E-TAN die Transaktionsnummern in Echtzeit immer wieder neu generiert. Während der Eingabe der Daten bei der Online-Transaktion generiert die Internet-Seite der Bank eine Kontrollnummer, die der Kunde in seine E-TAN-Box eingibt. Die E-TAN-Box erstellt darauf eine Antwort-Nummer, mit der der Kunde die Transaktion durchführen kann. Bei einer I-TAN (indizierte TAN) wird der Kunde von der Bank aufgefordert, eine bestimmte, durch eine Positionsnummer (Index) gekennzeichnete TAN aus seiner Liste einzugeben.

Trojaner (Trojanisches Pferd): Kombination eines (manchmal nur scheinbar) nützlichen Wirtsprogramms mit einem versteckt arbeitenden, bösartigen Teil, oft Spyware oder ein Backdoor (Hintertür). Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogramms für seine Installation durch den Benutzer.

Verschlüsselung: Vorgang, bei dem ein Klartext durch einen Verschlüsselungsalgorithmus und in der Regel geheimen Schlüssel in einen verschlüsselten Text umgewandelt wird.

Symmetrische Verschlüsselung: Für Ver- und Entschlüsselung wird derselbe Schlüssel verwendet.

Asymmetrische Verschlüsselung: Für die Verschlüsselung wird ein Public-Key (öffentlicher Schlüssel) verwendet und für die Entschlüsselung ein Private-Key (geheimer Schlüssel).

Voice over Internet Protocol (VoIP): (Telefonieren über das Internet. Die Sprachdaten werden in digitale Form umgewandelt, in kleinen Datenpaketen über das Internet verschickt und beim Empfänger wieder zusammengesetzt.

Würmer: siehe Computerwurm.

Zombie: Infiziertes Computersystem, das einen Teil eines BotNet bildet und durch C&C-Server kontrolliert wird.

Zugangsdaten: Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind.

Notizen