.BK
BUNDESKRIMINALAMT

CYBERCRIME

2012

Report

Impressum:
Herausgeber: Bundeskriminalamt, Josef-Holaubek-Platz 1,
1090 Wien;
Fotos und Grafiken: © Bundesministerium für Inneres (BM.I),
© Bundeskriminalamt (.BK), © Euopol, © Amy Walters – fotolia.
com, © a4stockphotos – fotolia.com;
Druck: Lepuschitz – Promotion, Peter Paul Straße 30,
2201 Gerasdorf / Wien;
Stand: September 2013

Moderne Kriminalitätsbekämpfung: Zeitgemäße Methoden

Aktuell prägen die technologischen Entwicklungen einer digitalisierten Welt die Erscheinungsformen der heutigen Kriminalität – das gilt im Besonderen für das Kriminalitätsphänomen Cybercrime.

Täter bedienen sich heutzutage ausgefeilter highlevel Technologien und nutzen das Internet als Tatbegehungsörtlichkeit um ihre kriminellen Machenschaften weltumspannend per Mausklick ausführen und damit unvorstellbare Profite erwirtschaften zu können.

Das Internet ist heute nicht nur Schauplatz für Betrugs- und Finanzmittelkriminalität, die Verbreitung von Kinderpornografie oder die Organisierte Kriminalität, sondern es bildet auch den sogenannten enabling factor für Terrorismus und jegliche Form gefährlicher Cyberattacken auf Behörden, Institutionen und Unternehmen. Cybercrime stellt auch die Unternehmen in der Privatwirtschaft vor immer größer werdende 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 aktuell in Sekundenbruchteilen von versierten Kriminellen durchgeführt werden, wobei die klassischen kriminalgeographischen Schauplätze durch den virtuellen Raum entgrenzt werden. Der Aktionsraum der Täter ist per Mausklick weltumspannend.

Psychologische Hemmschwellen schwinden, da die Straftäter ihren Opfern gar nicht mehr gegenübertreten müssen, was zu einer immensen Erweiterung des Täterspektrums in allen Kriminalitätsbereichen geführt hat. Die sogenannte Underground Economy steht den „Cybercrime-Anfängerinnen und -Anfängern" ebenso wie den Expertinnen und Experten quasi einem Online-Selbstbedienungsladen 24/7 zur Verfügung. Erforderliches fachliches Know-how, Tatbegehungsmittel für alle erdenklichen Zwecke und nicht zuletzt ein unüberschaubares Netzwerk von professionell miteinander in Verbindung stehender Berufsverbrecher, stellt das Internet bereit.

Eine völlig neue Sprache mit einem spezifischen Fachvokabular, das die Täter für ihre kriminellen Machenschaften benutzen, erschweren neben Verschlüsselungs- und Anonymisierungssoftware die Gefahrenabwehr und die Strafverfolgung durch Sicherheits- und Justizbehörden.

An adäquaten Antworten auf diese vielfältigen Bedrohungsphänomene des digitalen Zeitalters wird seitens der Rechtsstaaten sowohl auf nationaler als auch auf internationaler Ebene intensiv gearbeitet. Die Sicherheitsarchitektur verändert sich also, um mit der Innovationsgeschwindigkeit des modernen Technologiefortschrittes mithalten zu können.

Der vorliegende Cybercrime Report 2012 soll in diesem Zusammenhang einen Beitrag leisten, um aktuelle Entwicklungen, Phänomene und Herausforderungen und mögliche Tendenzen in diesem wichtigen Kriminalitätsfeld aufzuzeigen. Es ist unsere Bemühung diese neuen Kriminalitätsphänomene auf verständliche Art und Weise für die Leserinnen und die Leser darzustellen.

Wissen schützt! Das ist das Credo des österreichischen Bundeskriminalamtes. Diesem Leitspruch folgend gibt der vorliegende Cybercrime Report auf der Grundlage aktueller Daten, Zahlen und Fakten einen umfassenden Überblick über dieses wichtige Sicherheitsthema für Österreich.

Mag.ª Johanna Mikl-Leitner
Bundesministerin für Inneres

General Franz Lang
Direktor des Bundeskriminalamts

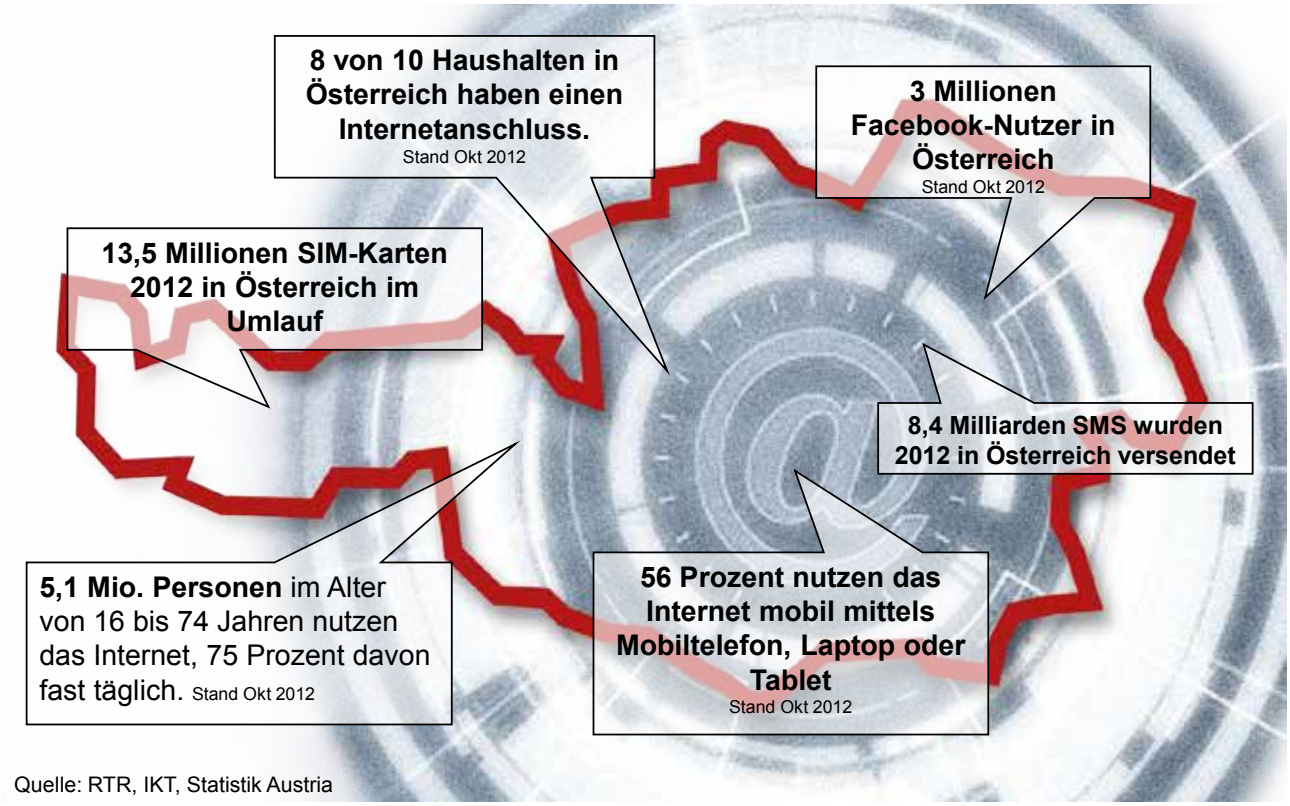
Der Inhalt: Das Verzeichnis

Der virtuelle Raum: Grenzenloser Kommunikations- und Marktplatz

Das Internet hat sich seit seiner Entstehung in vielen Entwicklungsphasen zu „dem" weltumspannenden Kommunikationsmedium entwickelt. Laut „Internet World Stats" gab es im Jahr 2000 bereits weltweit mehr als 361 Millionen Internetzugänge, bis zum Jahr 2012 ist diese Zahl auf über 2,4 Milliarden angestiegen.

Von den österreichischen Haushalten waren im Jahr 2012 bereits 79 Prozent mit einem Internetzugang versorgt. Als weltweiter Marktplatz ist das Internet für die heimische Wirtschaft unverzichtbar geworden. Nahezu alle österreichischen Unternehmen verfügen bereits über einen Internetzugang.

Die Bedeutung von Social Media Plattformen wie Facebook und Twitter ist weiter stark im Ansteigen und aus dem sozialen Leben vieler Menschen nicht mehr wegzudenken. Alleine Facebook, als bekannteste Social Media Plattform, erreichte in Österreich bis Ende 2012 rund drei Millionen registrierte Userinnen und User.



Neue mobile Geräte wie zum Beispiel Smartphone und Tablet-PC und die ständige Verfügbarkeit des Internets lassen uns am „virtuellen" Leben teilnehmen und verändern so Verhaltensmuster und Kommunikationsformen. Besonders bei Kindern und Jugendlichen zeigt sich der enorme Stellenwert des Internets. Das Einstiegsalter von Kindern und Jugendlichen in die virtuelle Welt ist dabei anhaltend sinkend.

Nahezu jeder österreichische Haushalt ist im Besitz zumindest eines oder mehrerer Mobiltelefone. 2012 gab es in Österreich rund 13,5 Millionen SIM-Karten. Damit ergibt sich eine auf die SIM-Karten bezogene Handydichte von 159 Prozent Im Vergleich zu 2011 ergibt das ein Plus von vier Prozent.

Der Anteil an Smartphones in Österreich ist dabei bis zum Jahr 2012 auf rund 60 Prozent angestiegen. Nicht zuletzt, weil immer mehr Kriminelle die Möglichkeiten dieser multifunktionalen

Geräte zu schätzen wissen, erlangen mobile Geräte auch in der polizeilichen Arbeit immer mehr an Bedeutung.

Cyberkriminalität: Eine Querschnittsmaterie

Was versteht man unter Cybercrime? Eine generell gültige Definition für Cybercrime gibt es nicht, allerdings wird hier im Allgemeinen Kriminalität unter Nutzung von Informations- und Kommunikationstechnik verstanden. Darunter fallen einerseits jene Delikte, 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 Kinderpornografie im Internet (§ 207a StGB). Cybercrime stellt somit eine Querschnittmaterie dar und 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. Das Phänomen des „Cyber-Groomings“ wurde zum Beispiel ab Januar 2012 durch den neugeschaffenen Paragraphen 208a Strafgesetzbuch (StGB) strafbar gemacht.

Zahlen und Fakten: Anstieg der Delikte

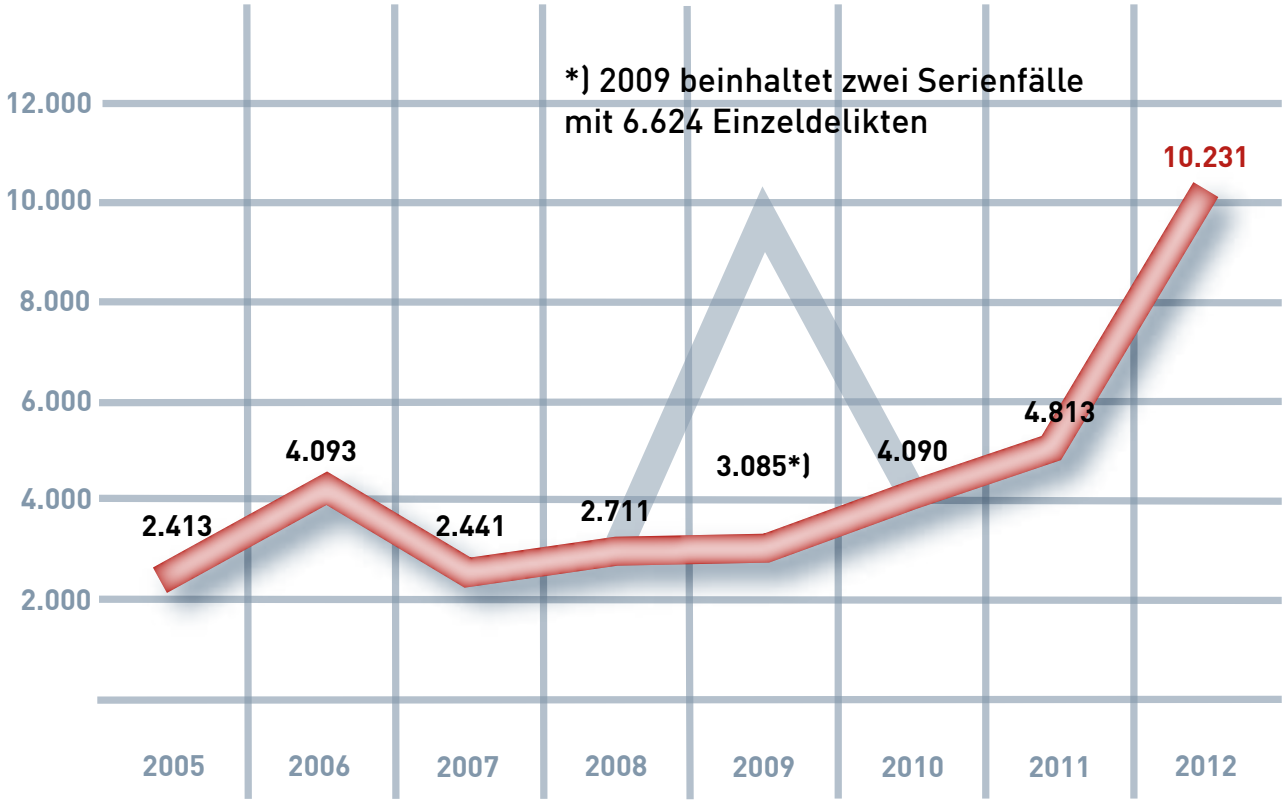
Da das Internet viel Raum für kriminelle Aktivitäten bietet, nehmen auch neue Bedrohungen aus dem Netz zu. Im Jahr 2012 war weltweit ein starker Anstieg der auf Mobiltelefone ausgerichteten Schadsoftware feststellbar. Außerdem spezialisieren sich Cyberkriminelle immer stärker auch auf soziale Netzwerke und verwenden diese für Betrugsversuche oder die Verbreitung von Schadsoftware.

Auch die weitere Steigerung von Betrugshandlungen im Internet hält 2012 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.

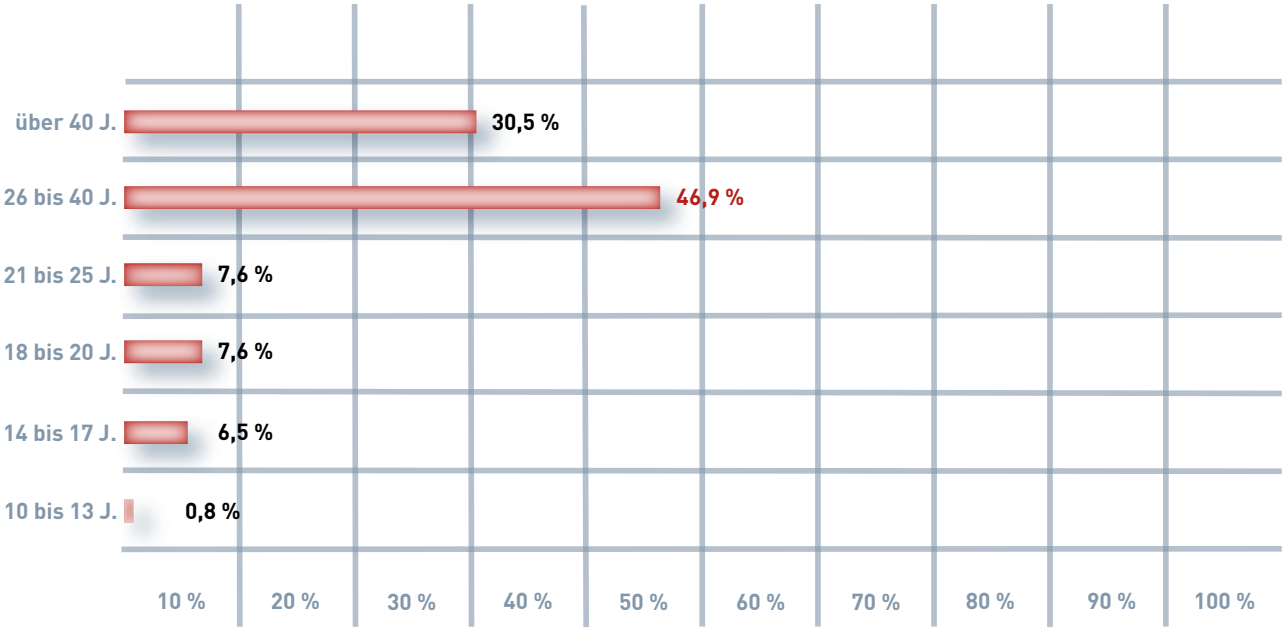
Das wahre Ausmaß des Schadens, der durch Cyberkriminelle verursacht wird, lässt sich nur schwer erfassen. Studien (Norton Cybercrime Report 2012) gehen von weltweit bis zu 1,5 Millionen Opfern von Cybercrime pro Tag aus. Dennoch dürfte die Dunkelziffer nach wie vor sehr hoch sein. Viele Betroffene erstatten 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 Cyberattacken bekannt zu machen.

Wie bereits in der Vergangenheit ist auch im Jahr 2012 ein weiterer Anstieg der IT-Kriminalität im Netz statistisch feststellbar.

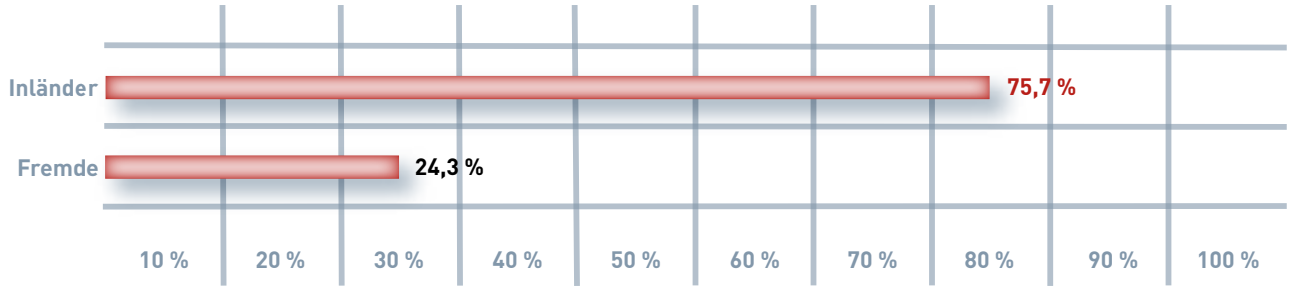


Die Aufklärungsquote lag 2012 durchschnittlich bei rund 25 Prozent, was einen Rückgang von rund 20 Prozentpunkten gegenüber 2011 bedeutet. Dies ist einerseits auf die immer stärkere Professionalisierung der Tätergruppierungen, die kriminell organisiert und international vernetzt sind, sowie den immer stärkeren Einsatz von Schadprogrammen zurückzuführen. Gleichzeitig wird die Ermittlungsarbeit bei Cybercrime-Delikten durch den Einsatz von Anonymisierungsdiensten und neue Technologien immer schwieriger und langwieriger.

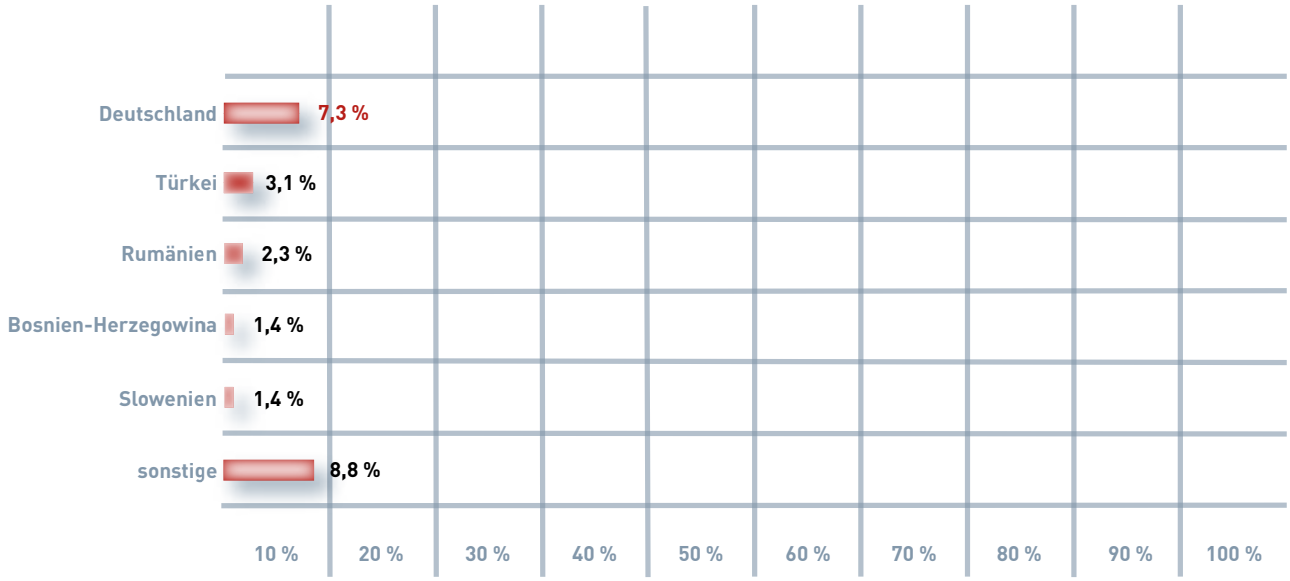
Bei den Tatverdächtigen ist mit rund 47 Prozent die stärkste Gruppe die der 25- bis 40-Jährigen (2011: 46 Prozent), gefolgt von den über 40-Jährigen mit rund 30 Prozent (2011: 28 Prozent).



Im Jahr 2012 stammten von den ermittelten Tätern rund 76 Prozent aus dem Inland.



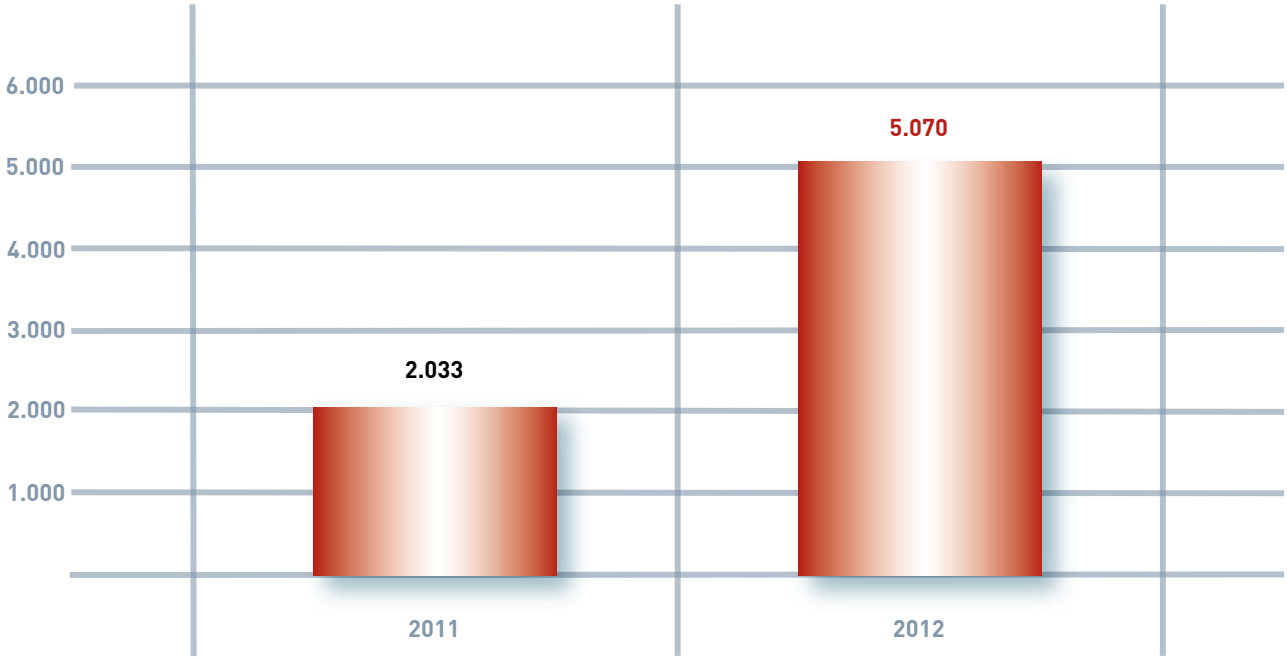
Der Anteil an Nicht-Österreicherinnen und Nicht-Österreichern beträgt rund 24 Prozent, wobei Deutschland mit rund sieben Prozent und Türkei mit rund drei Prozent den größten Anteil stellen. Hier wirkt sich die räumliche und sprachliche Nähe zu Deutschland, vor allem bei Betrugsfällen im Internet, aus. Ansonsten ist schwerpunktmäßig eine Verteilung der Täter im osteuropäischen Raum zu erkennen.



Internetkriminalität: Erscheinungsformen

1. Betrug mittels neuer Medien

Neue Medien nehmen einen immer größer werdenden Stellenwert in der Gesellschaft ein. Auch im Bereich der Kriminalität ist festzustellen, dass die neuen Medien immer stärker genutzt werden, um Betrügereien zu begehen. Einerseits bieten das Internet und die neuen Technologien den Tätern Anonymisierungsmöglichkeiten, eine größere Reichweite und eine schnelle Vorgehensweise unter Nutzung ständig wechselnder falscher Identitäten. Andererseits trägt der teilweise sorglose Umgang der Bevölkerung bei der Nutzung des Internets und der neuen Medien zusätzlich seinen Teil dazu bei. Vielfach agieren die Täter aus dem Ausland und verschleiern ihre Spuren, wodurch eine Nachverfolgung für die Strafverfolgungsbehörden in Österreich deutlich erschwert wird. Gerade im Bereich des Internetbetrugs kam es im Jahr 2012 zu einem starken Anstieg – konkret um 149,4 Prozent – im Vergleich zum Vorjahr.



Typischerweise werden beim Internetbetrug die neuen Medien zur Kontaktherstellung mit potentiellen Opfern benutzt. Das einzige Ziel der Täter ist die Erwirkung einer Geldleistung von den Opfern. Die Betrüger versuchen Sie mit vertrauensbildenden Maßnahmen, mit Überzeugungskraft oder Druck und unter Vorspielen von lebensnahen Sachverhalten alles Mögliche zu tun, damit das Opfer auf sie hineinfällt. Dabei differenziert man verschiedenste Erscheinungsformen. Eine komplette Aufzählung ist aufgrund der genutzten Betrugsschema und der sich ständig ändernden Vorgangsweise nicht möglich, wobei folgende Betrugsformen besonderes zu erwähnen sind:

Bestellbetrügereien

Beim Bestellbetrug gibt es zwei mögliche Vorgehensweisen: einerseits werden Waren mit dem Vorsatz bestellt, diese nicht zu bezahlen. Dabei werden falsche Namen angegeben beziehungsweise 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 Käufer bezahlen die Kaufsumme, erhalten jedoch die Waren nicht, da diese nie vorhanden waren bzw. nicht die Absicht bestand diese zu versenden. Bei der Vorgangsweise werden Techniken genutzt, um die Herkunft und Identität der Täter zu verschleiern und Serverstandorte in Ländern gewählt, die behördliche Ermittlungen erheblich erschweren.

„Lovescam“ oder „Datingscam“

Beim so genannten „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 Angabe eines einigermaßen lebensnahen Vorwandes 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. Der Vielzahl an Ideen der Betrüger ist hier keine Grenze gesetzt.

Finanzagenten oder Money Mules

Eine Person stellt als Finanzagent sein Konto den Tätern zur Verfügung, auf dem Gelder aus kriminellen Aktivitäten empfangen werden, um diese dann in weiterer Folge an andere Finanzagenten oder an die Täter weiter zu transferieren. Oftmals wird diese Tätigkeit als Nebenjob – seit einigen Jahren bevorzugt über neue Medien – angeboten. (Betreff: „Arbeit für dich“). Dabei wird dem Finanzagenten ein meist zweistelliger Prozentsatz des auf sein Konto transferierten Betrages als Gewinn versprochen. Die überwiesenen Gelder stammen dabei von Personen, die selbst Opfer krimineller, zumeist betrügerischer Handlungen wurden oder auch als Finanzagenten tätig sind. Der international als Money Mule bezeichnete 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 viele 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.

Arbeit für Dich!

Gut bezahlte Arbeit

Wir bieten Dir sehr gute Verdienstmöglichkeit!
Mit uns wirst Du einfach von 4.000 bis 8.000 Euro im Monat verdienen. Es gibt die Möglichkeit, die Arbeit bei uns mit Deinem jetzigen Job zu vereinbaren! Für diese Arbeit wirst Du nicht mehr als 2-3 Stunden pro Tag 1-2 Mal in der Woche aufwenden. **Für jeden ausgeführten Auftrag, der bei Dir nicht mehr als 3 Stunden in Anspruch nehmen wird, wirst Du von 400 bis 1.600 Euro verdienen.**

Gewinnversprechen

Mittels E-Mail, aber auch postalisch, werden Gewinnverständigungen versendet. Vor einer möglichen Inanspruchnahme des angeblichen Gewinns werden Überweisungen für die Freigabe des Gewinns sowie für diverse andere Zahlungen verlangt. Der vorgetäuschte Gewinn wird nie ausbezahlt.

Notfall-E-mails

Die Täter erlangen durch Hacking- oder Phishing-Attacken Zugangsdaten von Emailaccounts bei Freemailanbietern und übernehmen diese Konten. In weiterer Folge nutzen sie die in den Postfächern vorhandenen oder im Adressbuch gespeicherten Kontakte, schreiben diese an und spielen den Empfängern der Emails vor, dass der Nutzerin oder dem Nutzer des Accounts ein Notfall widerfahren ist. Das potentielle Opfer ist somit die Empfängerin bzw. der Empfänger der Nachricht. Dieser modus operandi hat zum Hintergrund die Hilfsbereitschaft auszunutzen und zielt rein auf die Erlangung einer Geldleistung zumeist mittels einem Zahlungsdienstleisters ab.

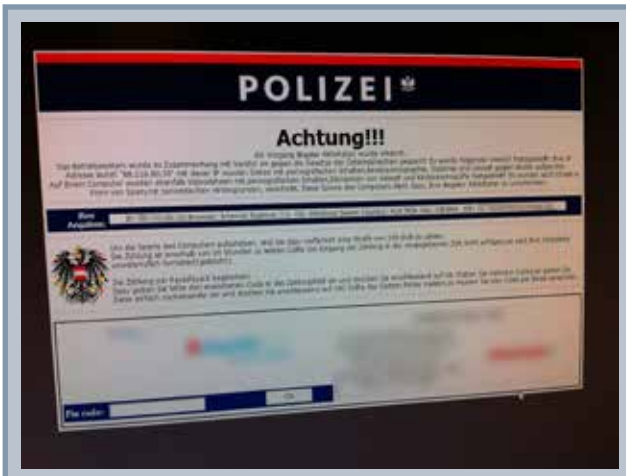
2. Viren, Würmer, Spyware, Trojaner-Programme

Schadprogramme wie Trojaner, Viren, Würmer, Spyware usw. werden in immer kürzeren Entwicklungszyklen und in immer größeren Mengen im Internet verbreitet. Das Gefahrenpotenzial dieser Schadprogramme ist erheblich und wird mitunter von der organisierten Kriminalität zur Durchführung von Straftaten eingesetzt. Hacker und Virenautoren arbeiten mit diesen Tätergruppen zusammen und schreiben spezielle Schadprogramme für Phishing, Kreditkartenbetrug und Erpressungsdelikte. Finanzielle Interessen sind dabei die ausschlaggebende Antriebskraft.

Der primäre Infektionsvektor hat sich dabei verlagert und erfordert nicht mehr das aktive Zutun der Benutzerin oder des Benutzers. Cyberkriminelle bedienen sich zunehmend Sicherheitslücken, um den Personal Computer (PC) beim Internetsurfen durch sogenannte Drive-By-Downloads zu infizieren.

Ein besonders starker Anstieg war 2012 bei den Vergehen gemäß § 126a Strafgesetzbuch (StGB) Datenbeschädigung von 70 Anzeigen im Jahr 2011 auf 296 Anzeigen im Jahr 2012 und bei § 126b StGB Störung der Funktionsfähigkeit eines Computersystems von acht im Jahr 2011 auf 645 im Jahr 2012 feststellbar.

Ursache für diesen ungewöhnlich starken Anstieg ist das weiterhin verstärkte Auftreten von sogenannter „Police-Ransomware“ – besser bekannt unter der Bezeichnung „Polizei-Virus“ oder „Polizei-Trojaner“ – in Österreich.



Das Bundeskriminalamt ermittelt seit dem Frühjahr 2012 gegen eine Tätergruppe, die mit der Verbreitung dieser „Ransomware“ im Internet aktiv ist. Dabei wird Schadsoftware verschickt, die Computersysteme sperrt und die Userinnen und User auffordert, für die Freigabe des PC Geld zu überweisen. Erste Varianten dieser Schadprogramme tauchten bereits 2005 auf, blieben jedoch nahezu ausschließlich auf Russland beschränkt. Die neueren Varianten verwenden unter anderem die Logos von verschiedenen Polizeibehörden. Von diesem Virus sind beispielsweise auch die Länder Spanien, Italien, Deutschland und die Niederlande betroffen. 2011 wurden schließlich erste Fälle bekannt, bei denen auch das Logo der österreichischen Polizei missbräuchlich verwendet wurde. In Österreich wurde die Schadsoftware unter der Bezeichnung „Polizei-Virus“ bekannt, wobei vorgetäuscht wird, dass sie von der Bundespolizei oder dem Bundeskriminalamt stammt. Sie wird beim Surfen auf manipulierten Webseiten automatisch und zum Teil ohne Zutun der Benutzerin oder des Benutzers auf dem Zielsystem installiert. Beim nächsten Start des Betriebssystems öffnet sich eine Seite mit einem Text, in dem behauptet wird, dass die Userin oder der User an strafbaren Handlungen beteiligt war und der Rechner deshalb von der Polizei gesperrt wurde. Nur gegen Zahlung eines Geldbetrages sei ein Entsperren des Computers möglich. Für die Entfernung der Schadsoftware finden sich mittlerweile im Internet zahlreiche hilfreiche Seiten, vor allem unter https://www.botfrei.de/ oder http://www.bka-trojaner.de/ sind entsprechende Informationen zum Entfernen der Schadprogramme zu finden. Die Ermittlungen gegen diese Tätergruppe laufen derzeit in mehreren europäischen Ländern und werden bei Europol analysiert und koordiniert.

Österreich gehört neben Deutschland, Italien, Frankreich, Spanien und Finnland zu den europaweit am stärksten betroffenen Ländern. Im Jahr 2012 sind mehr als 3.000 Anzeigen von Opfern an die zuständige Staatsanwaltschaft übermittelt worden.

3. BotNetzwerke

Durch die Verbreitung von Malware, wie zum Beispiel Trojaner, Würmer, usw. ist es Kriminellen möglich, die Kontrolle über fremde Rechner, so genannte „Zombie-Rechner", zu erlangen und diese in ein eigenes Netzwerk einzubinden. Diese Netzwerke bestehen zum Teil aus tausenden von übernommenen Rechnern, die über „Command and Control Server" („C&C-Server") ferngesteuert werden können. Mit solchen BotNetzwerken können nicht nur einzelne Rechner oder ganze Netzwerke durch „DDoS-Attacken" lahm gelegt werden, sondern sie dienen oft auch zur Versendung von Spam- und Phishingmails. Die Inhaber von Zombie-Rechnern sind meist unerfahrene Userinnen und User, die ihre Geräte unzureichend gegen Viren und Hackerangriffe gesichert haben. Seit Jahren ist weltweit eine Zunahme von BotNetzwerken zu verzeichnen. BotNetzwerke werden im Internet vertrieben oder überlassen, wobei im Bereich der Tätergruppen erhebliche Geldsummen gezahlt werden, was sich für die Täter wiederum durch die hohen Gewinne der damit begangenen Straftaten rechnet. Allerdings ist es den Strafverfolgungsbehörden zum Teil in Kooperation mit privaten Unternehmen gelungen, auch große BotNetze zu übernehmen oder auszuschalten. Hier zeigt sich deutlich, dass die Bekämpfung solcher Phänomene nur durch eine staaten- und bereichsübergreifende Kooperation erfolgreich ist. In den letzten Jahren zeigte sich auch, dass immer wieder Unternehmen in Österreich Ziel von DDos Attacken geworden sind.

Die Motivationen der Täter waren unterschiedlich, es wurden dabei auch nicht immer finanzielle Interessen verfolgt. Oft handelt es sich um bloße Racheakte von zum Beispiel gekündigten Mitarbeiterinnen oder Mitarbeitern oder Störaktionen von Konkurrenten. Für die Bekämpfung und Analyse von Aktivitäten von BotNetzwerken sind erhebliche personelle und technische Ressourcen erforderlich. Für die Ermittlungen sind die Kontakte zu ausländischen Dienststellen, im speziellen außerhalb Europas, von größter Bedeutung. Die Bekämpfung von BotNetzwerken stellt eine der großen polizeilichen Herausforderungen im Bereich der Internetkriminalität dar. Aus diesem Grund ist das österreichische Bundeskriminalamt ein aktives Mitglied in der „Interpol Working Party on Cybercrime", die sich mit der Bekämpfung dieses Phänomens befasst.

4. Phishing

Bei Phishing wird versucht, der Empfängerin oder dem Empfänger mittels einer E-Mail Zugangsdaten und Passwörtern zu entlocken. Meist erfolgt dies im Zusammenhang mit Online-Banking oder ähnlichen Zahlungssystemen. Zur Täuschung der Opfer werden Internetseiten von Bankinstituten täuschend ähnlich nachgeahmt, um die Empfängerinnen und Empfänger zur Bekanntgabe von Zugangsdaten zu bewegen. Seit längerem sind aber auch spezielle Softwarelösungen im Internet aufgetaucht, die unter Verwendung von Trojanerprogrammen und anderer Malware Zugangsdaten und Transaktionsinformationen vom Opfer unbemerkt an die Täter übermitteln. Diese Aktivitäten sind zum Beispiel unter der Bezeichnung „Man in the Middle" oder „Man in the Browser" bekannt geworden. Das Phänomen des Phishings beschäftigt die österreichische Exekutive bereits seit Ende 2005.

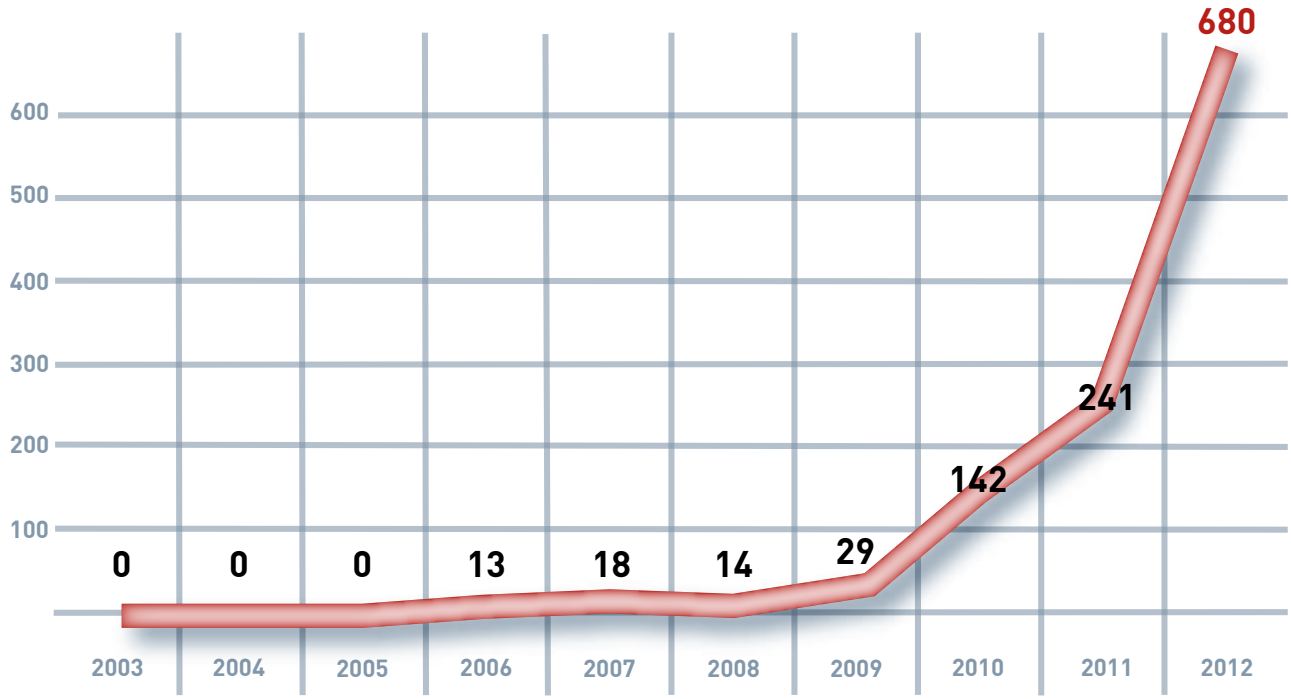
Ab Mitte des Jahres 2007 war in Österreich – entgegen den internationalen Trends – ein starker Rückgang von Phishingfällen feststellbar. Seit 2011 wird aber wieder ein Ansteigen der Anzeigen registriert, was vor allem auf neue Tätergruppen und neue Varianten von Trojaner-Programmen, die nunmehr auch in Österreich aktiv sind, zurückzuführen ist. Die angezeigten Fälle von Phishing sind von 184 Anzeigen im Jahr 2011 auf 394 Anzeigen im Jahr 2012 angestiegen.

5. 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. Als Motiv geben die Täter einerseits kriminelle Motive wie Betrugsabsicht oder andererseits Langeweile, Geltungsdrang oder Nachahmung an.

Wie bereits in den vergangenen Jahren war auch im Jahr 2012 ein starker Anstieg im Bereich des Hackings feststellbar. Während im Jahr 2011 noch 241 Fälle gemeldet wurden, sind diese im Jahr 2012 auf 680 Fälle angestiegen. Dabei wird Hacking häufig als Vorbereitungshandlung für andere Delikte zum Beispiel für den Diebstahl von Finanzdaten benutzt. Ursächlich für diesen Anstieg dürften eine verbesserte „Anzeigemoral" in der Bevölkerung infolge Medienberichterstattungen sowie die Zunahme von Hackingfällen in sozialen Netzwerken sein.



Im Frühjahr 2012 konnte vom Bundeskriminalamt ein 15-jähriger Hacker aus Niederösterreich ausgeforscht werden. In nur drei Monaten führte der Jugendliche 259 Hackerangriffe auf verschiedene in- und ausländische Unternehmen durch. Dazu suchte er im Internet gezielt nach Schwachstellen und Programmierfehler, um dann in die IT-Systeme einzudringen. Seine Hauptbeweggründe waren Langeweile und Geltungsdrang.

Telefonanlagen-Hacking

Besonders betroffen von Manipulation oder illegaler Verwendung von Telefonanlagen sind Klein- und Mittelbetriebe. Dabei werden Telefonanalagen in Unternehmen immer wieder von Hackern dazu benutzt, um Anrufe zu Mehrwertnummern oder ins Ausland zu tätigen. Meist erfolgen diese Angriffe an Wochenenden oder Feiertagen, wenn diese Firmen unbesetzt sind. Dabei wird häufig eine einfache Rufumleitung am System eingerichtet, die dann missbräuchlich durch die Täter verwendet wird. Der Schaden beläuft sich in den meisten Fällen auf mehrere tausend Euro und wird erst bei der Kontrolle der Abrechnungen festgestellt. Vom Missbrauch betroffen sind vor allem Telefonanlagen, bei denen das zur Administration bzw. Fernwartung vorgegebene Kennwort nicht geändert wurde.

Angriffe auf Social Media-Accounts

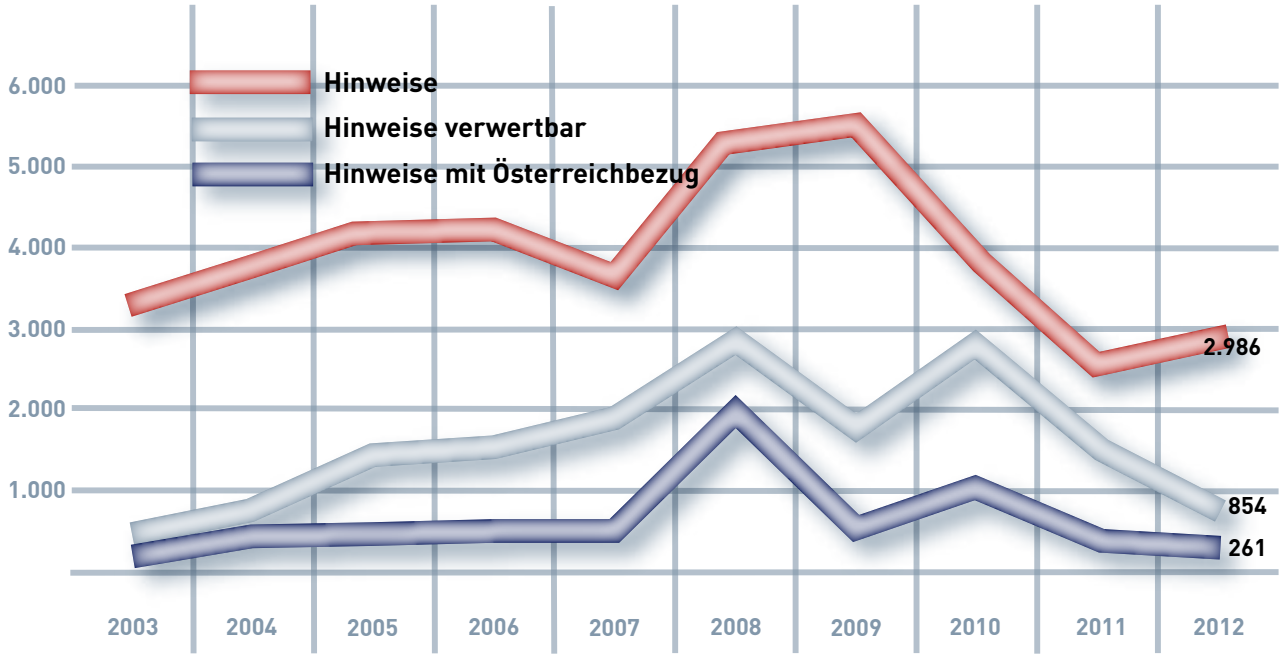
Soziale Netzwerke wie Facebook, Twitter usw. werden vor allem durch Malware, Hacker und Personen aus dem Lebensumfeld angegriffen. Ungeeignete Passwörter, zu viel Vertrauen, ein sorgloser Umgang mit Informationen und ein unbeschränkter Zugang zu den Profilen sind wichtige Parameter, die bei Attacken 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 durch Personen aus dem Lebensumfeld der Geschädigten oder des Geschädigten ausgeführt. 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.

6. Kinderpornografie

Kinderpornografie ist nach § 207a StGB geregelt, der besagt, dass die Herstellung, Verbreitung und der Besitz von pornografischen Darstellungen einer minderjährigen Person strafbar ist. Mit 1. Jänner 2012 wurde der neue § 208a StGB „Anbahnung von Sexualkontakten zu Unmündigen" eingeführt. Dieser gibt nunmehr auch einen Straftatbestand für Cybergrooming im österreichischen Strafrecht.

Laut der Kriminalstatistik Österreich ist die Zahl der Anzeigen von 502 Anzeigen im Jahre 2011 auf 543 im Jahre 2012 angestiegen. Im Jahr 2012 sind in der Meldestelle 2.986 Hinweise bearbeitet worden, wovon 261 Hinweise Österreichbezug aufwiesen.



Im Bereich des Kindersextourismus wurden im Jahr 2012 weitere Schulungen von Reiseveranstaltern durchgeführt bzw. die Zusammenarbeit mit den Behörden in den Zielländern intensiviert.

Informationen aus der internationalen Zusammenarbeit lassen auch Rückschlüsse auf einen Trend in der pädophilen Szene erkennen, wonach zunehmend Material aus sexuellen Mißbräuchen in Südostasien (Korea, Sri Lanka, Vietnam, Kambodscha etc.) verbreitet wird. Um diesem Trend zu begegnen wurden auch von Interpol die kriminalpolizeilichen Kontakte in die Zielländer verstärkt.

Unter der Leitung von Europol wurde 2012 das Projekt „HAVEN" (Halting Abusing Victims in Every Nation) weitergeführt. Im Rahmen dieses Projektes führt Europol eine gemeinsame Koordination zur effektiveren Bekämpfung von sexuellem Kindesmißbrauch, der von europäischen Staatsbürgern außerhalb ihrer Heimatländer begangen wird, durch. Ziel dieses Projektes

ist es, einerseits internationale, von EU-Strafverfolgungsbehörden geleitete Operationen zu koordinieren und andererseits durch Veranstaltungen und Kampagnen die Bevölkerung für diesen Deliktsbereich zu sensibilisieren. In Österreich wird das Projekt durch die Meldestelle für Kinderpornografie im Bundeskriminalamt betreut.

Meldestelle für Kinderpornografie und Kindersextourismus

Ein Schwerpunkt der Meldestelle im Jahr 2012 war wie schon in den Jahren zuvor, die Ausweitung von Kontakten zu gleichartigen Organisationseinheiten in den anderen Mitgliedsstaaten der Europäischen Union (EU) sowie zu Interpol und Europol.

Auch im Jahre 2012 wurde versucht, dem massiv anwachsenden Ausweichtrend der Szene auf Filesharingprogramme sowie „File hosting services" und Bulletin Boards zu begegnen und in diesem Bereich einen erhöhten Verfolgungsdruck zu erzeugen.

Die Beobachtung der Szene ergab im Jahr 2012 folgendes Lagebild:

- Das kommerzielle Angebot von kinderpornografischem Bildmaterial im World Wide Web ist weiter zurückgegangen. Dies ist auch im Rückgang der privaten Meldungen von Webseiten an die Meldestelle erkennbar.

- Durch die steigende Anzahl von Web 2.0-Anwendungen steht den Userinnen und Usern des Internets eine Vielzahl von sich stetig weiterentwickelnden Kommunikationsplattformen zur Verfügung, die zum Austausch von Informationen genutzt werden. Diese Entwicklung führte dazu, dass zwar die Anzahl kinderpornografischer Websites zurückgegangen ist, statt dessen aber das kinderpornografisches Material verstärkt auf Foren und Chats unter anderem in sozialen Netzwerken ausgetauscht wird.

- In diesem Zusammenhang wurde festgestellt, dass das TOR-Netzwerk im Bereich des Austausches von Daten mit kinderpornografischen Inhalten eine immer wichtigere Rolle spielt. Da es mit technischen Mitteln nicht möglich ist, etwaige Täter/Verdächtige festzustellen, bietet das TOR-Netzwerk eine ideale Möglichkeit zum „gefahrlosen" Datenaustausch. Die innerhalb des Netzwerkes existierenden „Hidden Services" – simple erstellte Homepages – werden hierbei als Plattform zum Austausch von Bildmaterial verwendet.

- Stark verbreitet ist nach wie vor das Angebot an – vordergründig legalen – „künstlerischen", „nudistischen" Aufnahmen von Kindern. Auch diese Anbieter werden, obwohl augenscheinlich nicht illegal, wie bereits in den vergangenen Jahren beobachtet, weil sich die Vermutungen verdichten, dass im geschlossenen Bereich dieser Websites sehr wohl kinderpornografisches Bildmaterial angeboten wird oder diese Kinder gar zum sexuellen Mißbrauch feilgeboten werden.

Die Cybercops: Im Team gegen die IT-Kriminellen

Die Bekämpfung von Cybercrime wird seitens der Exekutive auf allen Ebenen weiter verstärkt: auf lokaler Ebene in den Polizeiinspektionen und den Bezirks- und Stadtpolizeikommanden liegt der Fokus vor allem im Präventionsbereich sowie der Verbesserung der Ausbildungsmaßnahmen. Auf Ebene der Bezirke und der Landeskriminalämter erfolgten weitere Spezialisierungen und eine Bündelung des Know-hows. Mit der Einführung sogenannter Bezirks-IT-Ermittlerinnen und -ermitler wurde das Wissen in den einzelnen Dienststellen durch vor Ort verfügbare Expertinnen und Experten verbessert. Auf Bundesebene wird derzeit das Cybercrime-Competence Center, kurz C^4 genannt, eingerichtet.

Die Anforderungen an die Polizeibeamtinnen und –beamten werden gerade durch das rasch wechselnde Umfeld im Bereich Cybercrime ständig höher. Für eine effiziente Bekämpfung von Cybercrime sind daher neben einer modernen technischen Ausstattung vor allem gut ausgebildete Beamtinnen und Beamte auf allen polizeilichen Organisationsebenen erforderlich. Denn der Faktor Mensch spielt eine besondere Rolle, zunehmend wird bei komplexen oder schwierigen Ermittlungsfällen im Internet ein spezielles kriminalpolizeiliches Know-how erforderlich.

Weiter Ausbilden

Wie bereits in den vergangenen Jahren nahm auch im Jahr 2012 das Thema Aus- und Weiterbildung der Polizistinnen und Polizisten im Bereich IT-Kriminalität einen wichtigen Stellenwert in der gesamten Sicherheitsstrategie des Bundesministeriums für Inneres (BM.I) ein.

Die Polizistinnen und Polizisten auf der Ebene der Polizeiinspektionen, der Stadtpolizeikommanden und der Bezirkspolizeikommanden erhielten und erhalten im Rahmen ihrer Grundausbildung, bei ihrer Ausbildung zur dienstführenden Beamtin oder zum dienstführenden Beamten sowie im Rahmen von Fortbildungsmaßnahmen eine Basisschulung zum Thema IT-Kriminalität.

Neben zahlreichen Spezialschulungen für operativ tätige Kriminalbeamtinnen und –beamte fand 2012 die Grundausbildung der ersten Bezirks-IT-Ermittlerinnen und -Ermittler statt. Diese sind auf Bezirksebene Ansprechpartner für die Bevölkerung. Dabei handelt es sich um speziell ausgebildete Polizeibeamtinnen und -beamte, die im jeweiligen Landeskriminalamt (LKA) eine Zusatzausbildung und eine damit verbundene Praxisschulung erhalten haben. Sie unterstützen das jeweilige LKA bei der Datensicherung auf lokaler Ebene und nehmen bei Amtshandlungen, bei denen der Verdacht auf Cybercrime besteht, die richtigen Erstmaßnahmen vor, um den Tatort fachgerecht abzusichern und um den IT-Ermittlungsexpertinnen und -experten in den LKA sowie beim Bundeskriminalamt die anschließende Ermittlungsarbeit zu erleichtern. Da sich dieses Konzept der Bezirks-IT-Ermittlerteams gut bewährt hat, wurde 2012 begonnen diese wichtige Funktion bei allen Landeskriminalämtern österreichweit flächendecken einzuführen: im Jahr 2012 absolvierten mehr als hundert Ermittlerinnen und Ermittler das Basisausbildungsmodul im Bundeskriminalamt, in den Jahren 2013 und 2014 werden weitere folgen.

Auf lokaler und regionaler Ebene sind geschulte Präventionsbeamtinnen und -beamte insbesondere für Klein- und Mittelbetriebe aber auch für die fachkundige Information der Bevölkerung in Österreich im Einsatz. Darüber hinaus wird das Thema Cybercrime auch im Rahmen der Kriminaldienstfortbildungsrichtlinie (KDFR) behandelt. Die Vortragenden rekrutieren sich bei diesen KDFR-Schulungen sowohl aus den behördeneigenen IT-Expertinnen und –Experten bei den Landeskriminalämtern und beim Bundeskriminalamt wie auch durch externe Spezialistinnen und Spezialisten.

Auf Länderebene sind in den Landeskriminalämtern speziell ausgebildete Kriminalbeamtinnen und –beamte tätig. Diese sind in den Themenbereichen IT-Forensik und IT-Ermittlung ausgebildet

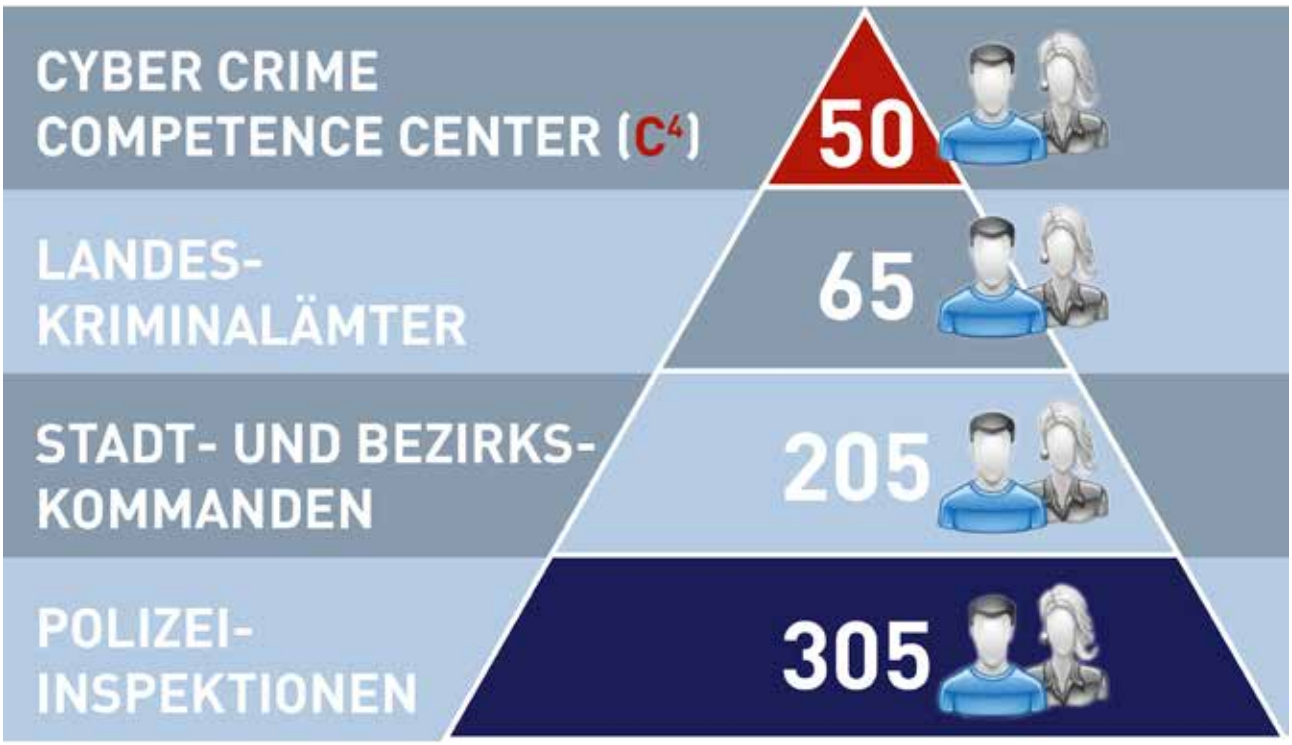
und arbeiten mit den Fachabteilungen der unterschiedlichen Ermittlungsbereiche an der Aufklärung von Internetkriminalität und Computerstraftaten durch fachliche Expertise und Spezialwissen mit.

Die Aus- und Fortbildung sowohl dieser Kriminalistinnen und Kriminalisten in den Landeskriminalämtern als auch jener im C^4 im Bundeskriminalamt ist vielseitig: regelmäßig werden sowohl behördeninterne Schulungs- und Fortbildungsveranstaltungen als auch Ausbildungen durch externe Expertinnen und Experten aus der Wirtschaft, wie zum Beispiel durch namhafte Softwareherstellerfirmen, abgehalten. Die Ausbildungsveranstaltungen bedienen ein breites Spektrum an informations- und kommunikationstechnisch (IKT)-relevanten Wissens für die IT-Kriminalitätsbekämpfung: beginnend bei Schulungen im Bereich Betriebssysteme und Auswertungssoftware bis hin zu Server und Netzwerke. Anlassbezogen finden beispielsweise auch Trainings mit dem Computer Emergency Response Team (CERT) statt.

Darüber hinaus nehmen die Beamtinnen und Beamten der IT-Ermittlungsbereiche auf Bundesebene (Bundeskriminalamt und Bundesamt für Verfassungsschutz und Terrorismusbekämpfung) auch an Ausbildungs- und Fachtagungen im Rahmen internationaler Seminare und Schulungen teil.

Internationale Organisationen, wie zum Beispiel die „International Association for Computer Information Systems“ (IACIS), ein Zusammenschluss von polizeilichen IT-Forensikerinnen und -Forensikern, führen Kurse im Rahmen europäischer Schulungsprojekte durch. Darüber hinaus war das Bundeskriminalamt vertreten durch das C^4 im Jahr 2012 am europäischen Schulungsprogramm „European Cyber Crime Training and Education Group“ (ECTEG) im Bereich „high-tech crime“ beteiligt. Weiters konnte im abgelaufenen Berichtszeitraum die bereits in der Vergangenheit sehr gute Kooperation mit nationalen Hochschulen weiter intensiviert und sehr erfolgreich fortgeführt werden.

Im Endausbau 2014 werden für Österreich folgende IT-Cops zur Verfügung stehen:



C⁴: Das Headquarter

CYBER CRIME
COMPETENCE CENTER

Im Jahr 2012 wurde mit der Umsetzung der Cybercrime-Strategie im BMI begonnen. Zentraler Bestandteil der Gesamtstrategie Cybercrime ist die Errichtung des Cybercrime-Competence-Centers, kurz C⁴, im Bundeskriminalamt als nationale und zentrale Koordinierungsstelle zur Bekämpfung von Cybercrime.
Das C⁴ bildet die Schnittstelle zu den Zentralstellen in den anderen Ländern sowie zum „European Cyber Crime Centre" (EC3) bei Europol und zum „Digital Crime Center" (IDCC) bei Interpol. Bestehende Kooperationen mit Wirtschaft und Forschung werden für einen weiteren Wissenstransfer ausgebaut.

Das Cybercrime-Competence-Center wird neben den kriminalpolizeilichen Aufgabenstellungen vor allem die Funktion einer zentralen nationalen und internationalen Schnitt- und Meldestelle sowohl innerhalb der polizeilichen Organisation als auch für Bürgerinnen und Bürger übernehmen.

Das C⁴ weist folgende Organisationsstruktur auf:

Cybercrime-Competence-Center C⁴

Meldestelle against-cybercrime@bmi.gv.at
Meldestelle für Cybercrime im Internet
Zentrale nationale und internationale Ansprechstelle im Zusammenhang mit Cybercrime

Referat Zentrale Aufgaben	Referat Support	Referat Ermittlungen
Prävention Ausbildung Analyse und Schnittstelle zu Wirtschaft und Forschung Technik	IT-Forensik Mobile Forensics	Ermittlungen in Netzwerken und bei speziellen Cyber-Crime Delikten wie z. B. Hacking, BotNetzen oder DDoS sowie Koordinierung von Großfällen Rasterfahndung

Die Aufgaben

1. Ansprechstelle für Betroffene

Im Mai 2011 wurde die Meldestelle „against-cybercrime@bmi.gv.at" im Bundeskriminalamt eingerichtet. Hier können Bürgerinnen und Bürger verdächtige Wahrnehmungen im Internet rund um die Uhr via E-Mail melden. Wurden im Jahr 2011 noch rund 1.300 Meldungen zu Vorfällen im Internet an diese Stelle gemeldet, so waren es 2012 bereits 6.341 Eingänge, was fast einer Verfünffachung entspricht.

Die eingemeldeten Sachverhalte betreffen vor allem Internetbetrugsfälle mit eher geringen Schadenssummen, betrügerische „Lockangebote", Hinweise auf Internetseiten oder der

Absenderin bzw. dem Absender verdächtig erscheinende Massenmails, die an Postfächer privater Personen gesendet wurden (419er-Briefe, Lotteriegewinne, etc.).

2. Erfassung, Analyse und Auswertung digitaler Spuren

Die Spezialistinnen und Spezialisten in den Landeskriminalämtern und des C4, die so genannten IT-Forensikexpertinnen und -experten, werden immer dann aktiv, wenn besondere Fälle von Computerkriminalität aufzuklären sind bzw. arbeiten unterstützend wenn polizeiliche Ermittlungen und technische Erhebungen erforderlich sind oder elektronische Beweismittel gesichert und ausgewertet werden müssen. Sie unterstützen somit in einem weiten Bereich die Exekutivbeamtinnen und -beamten bei ihren Ermittlungen, wie zum Beispiel gegen Kinderpornografie, Erpressungen, Eigentumsdelikten, Schlepperei und Menschenhandel. Dabei gelangen international anerkannte Methoden und best practices zum Einsatz. Standardmäßig stehen ihnen dafür eine spezielle Hardwareausstattung sowie verschiedene Forensik-Programme zur Verfügung. Durch den zunehmenden Einsatz von Smartphones ergeben sich sowohl für die Strafverfolgungsbehörden als auch für Kriminelle neue Möglichkeiten. Für die Auswertung von mobilen Geräten gelangt bei der Datensicherung und -aufbereitung eine spezielle Hard- und Software zum Einsatz. Besonders bei den mobilen Geräten, insbesondere Smartphones, war in den letzten Jahren ein starker Anstieg der Auswertungsersuchen aus nahezu allen Bereichen feststellbar. Im Bereich der elektronischen Beweissicherung stellen die ständig steigenden Datenmengen eine besondere Herausforderung dar. Das Phänomen der „Massendaten" erfordert eine stetige Ressourcenanpassung bei den Ermittlungsbehörden, ein Ende dieser Entwicklung ist nicht in Sicht.

3. Vernetzt 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 weiter intensiviert und ausgebaut wurden. 2012 wurden folgende Initiativen erfolgreich gestartet bzw. umgesetzt:

- **Projekt „IT-Sicherheit":** Dieses Projekt läuft bereits seit mehreren Jahren und soll einen rascheren Informationsausaustausch zwischen dem Bundesministerium für Inneres und der Wirtschaftskammer Österreich (WKO) erzielen. Wirksame Maßnahmen zur IT- und Datensicherheit für heimische Unternehmen werden immer wichtiger, da das Gefahrenpotential von Cyberattacken ständig zunimmt. Dazu wurde ein Informationsfolder erstellt und eine Internetplattform sowie IT-Sicherheitshandbücher von der WKO zur Verfügung gestellt. Auf der Internetplattform „IT-Safe" werden in Echtzeit Warnmeldungen des Bundeskriminalamts eingestellt, um so die Information möglichst rasch und zielgerichtet an die österreichischen Unternehmen weiter zu gegeben.
  Mehr Informationen finden Sie unter www.it-safe.at

- **Konferenz „Neue Technologien" - Internationaler Austausch mit Expertinnen und –experten aus Wirtschaft, Wissenschaft und Forschung:** Das österreichische Bundeskriminalamt veranstaltet gemeinsam mit dem Deutschen Bundeskriminalamt, dem Landeskriminalamt Bayern sowie dem Schweizer Bundesamt für Polizei (FedPol) jährlich die Konferenz „Neue Technologien". 2012 fand diese Veranstaltung in Bayern statt. Ziel dieser international anerkannten Expertenkonferenz ist es, innovative Projekte und Technologien mit polizeilicher Relevanz vorzustellen und eine Brücke zwischen Wissenschaft, Forschung und Polizei zu schlagen. Renommierte Organisationen und Forschungsinstitute haben hier bereits innovative Projekte und Forschungsergebnisse vorgestellt und so einen Blick in die zukünftige Entwicklung von „neuen" Technologien und der zukünftigen polizeilichen Arbeit ermöglicht. Weiters besteht mit dem deutschen Bundeskriminalamt eine Zusammenarbeit im Bereich des Technologieradars, wo aktuell technologische Entwicklungen auf ihre Relevanz in Bezug auf Nutzen und Gefahren für die Userinnen und User und die polizeiliche Arbeit geprüft und beurteilt werden.

- **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. Neben den regelmäßigen Weiterbildungsveranstaltungen in Bezug auf neue IT-Entwicklungen werden die IT-Forensikerinnen und -Forensiker des Bundeskriminalamts auch zu internationalen Schulungsaktivitäten wie zum Beispiel der „European Cyber Crime Training and Education Group" (ECTEG) entsandt. In dieser bei Europol angesiedelten Arbeitsgruppe werden auf europäischer Ebene Trainingsprogramme für IT-Forensik und IT-Ermittlungen erstellt und weiter entwickelt.

- **Internationaler Austausch:** Das Medium Internet selbst kennt keine Landesgrenzen. Daher muss die kriminalpolizeiliche Arbeit bei der Bekämpfung von Internetkriminalität auch auf dieser Ebene stattfinden. In Europa hat die EU bereits verschiedene Initiativen zur Eindämmung der Cyberkriminalität ergriffen. Trotz dieser Fortschritte stehen einer effizienten Bekämpfung von Cyberstraftaten und einer wirksamen Verfolgung der Täter weltweit immer noch Hindernisse wie zum Beispiel mangelnde Strafbarkeit, unzureichende Möglichkeiten für den Austausch von Erkenntnissen, technische Probleme bei der Ermittlung der Täterherkunft oder der Mangel an Fachpersonal entgegen. Um diesen Herausforderungen zu begegnen, hat die Europäische Kommission (EK) entschieden, ein Europäisches Zentrum zur Bekämpfung von Cyberkriminalität bei Europol einzurichten. Zudem werden in vielen Staaten ebenfalls vernetzte Zentralstellen errichtet. Das neu zu errichtende „European Cyber Crime Centre" (EC3) bei Europol spielt bei der Bekämpfung von Cybercrime eine wichtige Rolle. Es ist das Bindeglied zwischen den europäischen Ländern bei der Bekämpfung dieser Kriminalitätsform. Das EC3 wird die europäischen Staaten bei der Bekämpfung von Cybercrime unterstützen und die gemeinsamen Aktivitäten koordinieren. Interpol errichtet derzeit ebenfalls ein „Digital Crime Center" (IDCC) in Singapur. Das IDCC wird sich aktuellen Hightech-Fragen sowie der Verbesserung der Zusammenarbeit zwischen den Strafverfolgungsbehörden bei Cybercrime-Delikten widmen.

- **European Cyber Crime Task Force (EUCTF):** Im Rahmen der regelmäßig bei Europol veranstalteten EUCTF Meetings treffen sich die Leiter der Cybercrime-Units aus allen EU-Ländern. Dabei werden Erfahrungen und Know-How ausgetauscht, aktuelle Bedrohungen analysiert, neue Technologien vorgestellt und europaweite Lösungen und Strategien zur Bekämpfung von Cybercrime erarbeitet. In diesem Gremium ist auch das Bundeskriminalamt vertreten. Darüber hinaus nimmt das Bundeskriminalamt an operativen Meetings von Europol und Interpol teil. Hier werden in Analyse- oder Arbeitsgruppen Ermittlungserkenntnisse bei der Bekämpfung von Cybercrime zwischen den Expertinnen und Experten ausgetauscht und koordinierte Vorgangsweisen festgelegt.

Für Bürgerinnen und Bürger: So hilft die Polizei

Wer feststellt, dass sein Computer manipuliert wurde, wem Computerkriminelle das Konto leer räumen oder wer bei einer Internetauktion betrogen wurde, sollte gleich zur Polizei gehen. Eine Strafanzeige nimmt jede Polizeidienststelle entgegen. Darüber hinaus kann auch rund um die Uhr die Meldestelle im Bundeskriminalamt unter against-cybercrime@bmi.gv.at kontaktiert werden.

Die Polizei nimmt die Anzeige auf

Bei Bedarf untersucht die Polizei den PC oder macht eine Kopie von der Festplatte. Die IT-Forensikerinnen und -Forensiker werten die vom PC automatisch mitgeschriebenen Protokolle, die so genannten Log Files, aus und stoßen so oftmals auf die Spuren der Täter. Sie sichern die Beweismittel, etwa Hinweise aus E-Mails, News-Postings oder Beiträge auf Homepages. Außerdem können die Staatsanwaltschaft und die Kriminalpolizei vom Netzbetreiber oder von der Telefongesellschaft Informationen im Zusammenhang mit dem Datenverkehr anfordern. Daraus lässt sich ablesen, wer wann und mit welcher Computerkennung im Netz unterwegs war. Anhand dieser IP-Adresse kann die Polizei den Täter oftmals identifizieren und lokalisieren. Auch der Nickname oder andere Hinweise können zur Ermittlung des Täters führen.

Prävention und Information

Für die Polizei hat beim Thema „IT-Sicherheit" die Prävention einen hohen Stellenwert. Durch verstärkte, kompetente und rasche Präventionsarbeit kann viel zur Sicherheit jedes einzelnen im Internet beigetragen werden. Denn viele Betrugshandlungen und Angriffe auf IT-Systeme könnten bei entsprechender Aufmerksamkeit und adäquaten technischen Schutzvorkehrungen verhindert werden.

In vielen Veröffentlichungen und Veranstaltungen liefert die Kriminalprävention für die Firmen, Bürgerinnen und Bürgern konkrete Handlungsempfehlungen, die zu mehr Sicherheit beim Umgang mit Datenverarbeitungssystemen beitragen. So beteiligen sich die Expertinnen und Experten des Bundeskriminalamts mit aktiven Beiträgen bei Veranstaltungen, wie zum Beispiel bei jenen des Kuratoriums Sicheres Österreich (KSÖ) und der Wirtschaftskammer Österreich und unterstützen die Initiativen wie „SaferInternet", um so die jeweiligen Zielgruppen unmittelbar zu erreichen und dort das Verständnis für die Gefahren die mit der Verwendung des Internets und der sozialen Medien verbunden sind, zu verbessern. Ein Schwerpunkt der polizeilichen Vorsorgeaktivitäten ist die Information über technische Schutzmaßnahmen.

Beratung im Internet

Auf der Webseite und auf den Facebook-Seiten des Bundeskriminalamts gibt die Polizei Tipps wie man sich selbst und seinen Computer im Internet schützen kann und informiert über aktuelle Gefahren und Schutzmaßnahmen:
www.bundeskriminalamt.at oder www.facebook.com/bundeskriminalamt

Beratungsstellen vor Ort

Bei Fragen zum Thema Computerkriminalität können sich Bürgerinnen und Bürger als auch Unternehmen direkt an eine der Kriminalpräventionsstellen in ganz Österreich wenden. Diese stehen kostenlos unter der Nummer 059-133 für eine kompetente Beratung zur Verfügung.

„Click und Check“: Ein Jugendpräventionsprojekt der Polizei

Ein besonderer Schwerpunkt der Kriminalprävention wird auf die Zielgruppe der Kinder und Jugendlichen gelegt.

Pubertierende sind oft unbekümmert und neugierig, benötigen Aufmerksamkeit und Anerkennung, wünschen Freiheit, suchen Orientierung und versuchen, ihre Identität auszubilden. Und dies erfolgt immer öfters über das Medium Internet. Dabei können sie zum Täter, aber auch zum Opfer werden. Die Erwachsenen hingegen unterschätzen oft die Risiken. Information und Prävention – und das bereits ab dem Kindesalter – ist die einzige Möglichkeit, um unsere Kinder zu problem- und verantwortungsbewussten Erwachsenen zu machen.

Auf Polizeiebene wird derzeit bereits sehr erfolgreich

das Projekt „Click & Check“ umgesetzt. Dabei informieren eigens geschulte Polizeibeamtinnen und –beamte Jugendliche in den Schulen über „Happy slapping und „Cyberbullying oder –mobbying“ und versuchen anhand kurzer Videofilme das Unrechtsbewusstsein von Jugendlichen zu fördern und Gesetzesinformationen zu vermitteln. Im Jahr 2012 wurden österreichweit über 41.690 Kinder und Jugendliche über den richtigen, sicheren Umgang mit Handy und PC sensibilisiert und informiert.

Kriminalprävention in den Landeskriminalämtern

Landeskriminalamt Burgenland
Kriminalprävention
Neusiedler Str. 84
7000 Eisenstadt
Tel.: 059133/10/3750
E-Mail: LPD-B-LKA-Praevention@polizei.gv.at

Landeskriminalamt Kärnten
Kriminalprävention
Buchengasse 3
9020 Klagenfurt
Tel.: 059133/20/3750
E-Mail: LPD-K-LKA-Praevention@polizei.gv.at

Landeskriminalamt Niederösterreich
Kriminalprävention
Schanze 7
3100 St.Pölten
Tel.: 059133/30/3750
E-Mail: LPD-N-LKA-Praevention@polizei.gv.at

Landeskriminalamt Oberösterreich
Kriminalprävention
Gruberstraße 63
4021 Linz
Tel.: 059133/40/3750
E-Mail: LPD-O-LKA-Praevention@polizei.gv.at

Landeskriminalamt Salzburg
Kriminalprävention
Alpenstraße 88-90
5020 Salzburg
Tel.: 059133/50/3750
E-Mail: LPD-S-LKA-Praevention@polizei.gv.at

Landeskriminalamt Steiermark
Kriminalprävention
Strassgangerstraße 280
8052 Graz
Tel.: 059133/60/3750
E-Mail: LPD-ST-LKA-Praevention@polizei.gv.at

Landeskriminalamt Tirol
Kriminalprävention
Innrain 34
6020 Innsbruck
Tel.: 059133/70/3750
E-Mail: LPD-T-LKA-Praevention@polizei.gv.at

Landeskriminalamt Vorarlberg
Kriminalprävention
Bahnhofstraße 45
6900 Bregenz
Tel.: 059133/80/3750
E-Mail: LPD-V-LKA-Praevention@polizei.gv.at

Landeskriminalamt Wien
Wasagasse 22
1090 Wien
Tel.: 0800/216346
E-Mail: LPD-W-LKA-AB-Kriminalpraevention@polizei.gv.at

Kriminalpolizeiliches Beratungszentrum
Andreasgasse 4
1070 Wien
Montag bis Freitag, 9.00 bis 16.00 Uhr
Tel.: 01/31310/44938
E-Mail: LPD-W-LKA-AB-Kriminalpraevention@polizei.gv.at

Ein Blick in die Zukunft

Weltweit verfügen oder erhalten immer mehr Menschen Zugang zum Internet, die Verbreitung von mobilen Endgeräten erleichtert Waren und Dienstleistungen via Internet immer und überall zu bestellen und zu bezahlen. Es ermöglicht Kontakte zu knüpfen, alltägliche Geschäfte werden mehr und mehr elektronisch abgewickelt und auch im Rahmen des E-Governments immer weiter ausgebaut. Dadurch ist es für die Täter leicht möglich, auf einfache Art und Weise immer mehr Menschen in kürzester Zeit zu erreichen.

Es bestätigt sich daher der Trend der Vorjahre und es ist davon auszugehen, dass die bestehenden Erscheinungsformen weiter zunehmen werden, aber auch neue Erscheinungsformen vor allem bei den mobilen Endgeräten entstehen. Dies beinhaltet auch neue Technologien wie beispielsweise Near Field Communication (NFC) oder den Einsatz von QR-Codes zur Zahlungsdurchführung, die in den nächsten Jahren vermehrt Einzug halten werden und mögliche Betrugsszenarien diesbezüglich noch nicht abschätzbar erscheinen lassen. In allen diesen Bereichen wird insbesondere durch intensive Präventionsarbeit entgegenwirken zu sein.

Neuer Herausforderungen bringen auch das Darknet (engl. für „Dunkles Netz“) und das Deepweb mit sich. Beide werden seit Jahren von Kriminellen in den verschiedensten Bereichen zur Begehung von Straftaten benützt. Gewerbsmäßige, organisierte Kriminalität nützt diese in der Öffentlichkeit wenig bekannte Art und Weise der Kommunikation zum Beispiel in den Bereichen Internet Kinderpornografie, Kreditkartenbetrug aber auch die Suchmittelkriminalität verzeichnet signifikante Anstiege der Tatbegehungen im Darknet und Deepweb.

Informationstechnik im Alltag

Neue Informationstechniken durchdringen immer mehr unseren Alltag. So zielen zum Beispiel aktuelle Entwicklungen im Bereich der Verkehrstelematik darauf ab, unsere alltägliche Nutzung von Kraftfahrzeugen effizienter und sicherer zu machen. So können zum Beispiel Informationen zur lokalen Außentemperatur, der Luftfeuchtigkeit und der Fahrbahnoberfläche in jedem Kraftfahrzeug (Kfz) erfasst und mit den momentanen GPS-Positionsdaten verknüpft an eine zentrale Verarbeitungsstelle gemeldet werden. Mittels dieser Daten ist es nun möglich, orts- und zeitspezifischen Glatteiswarnungen zu erzeugen und automatisch an alle Fahrzeuge in der betroffenen Region weiterzuleiten. Ein weiterer Anwendungsfall ist die Meldung einer Vollbremsung an alle nachfolgenden Fahrzeuge, um so durch eine automatisch erfolgende Vorbremsung die Reaktionszeit und damit den Bremsweg aller in Kolonne befindlichen Kfz zu verkürzen. Um diese Aufgaben zu bewerkstelligen ist sowohl die Kommunikation einzelner Fahrzeuge untereinander als auch die von Fahrzeugen mit zentralisierten Diensten unabdingbar. Genau hier entsteht nun ein potentieller Ansatzpunkt für gezielt schädigendes und kriminelles Verhalten. So wäre es denkbar, dass durch die gezielte Manipulation übermittelter Daten gezielt Staus herbeigeführt werden könnten, oder noch schlimmer, einzelne Fahrzeuge in Funktion und Fahrverhalten von außen derart beeinflusst werden könnten, dass schwere Unfälle die Folge wären.

Sonnen- und Schattenseiten

Ein weiteres Beispiel findet sich im Cloud Computing: Dieser Begriff bezeichnet ein Konzept im IT-Kontext, in dem Dienstleistungen wie Berechnungsoperationen oder Datenspeicher aber auch ganze Anwendungsprogramme im Netzwerk flexibel verteilt, für die Benutzerin und den Benutzer aber scheinbar lokal und somit einfach zugreifbar gemacht werden. Was nun auf der einen Seite Komfort und Kostenflexibilität für die Anwender bedeutet, birgt allerdings auch Risiken im Bereich Sicherheit und Datenschutz. Durch die verteilte Natur von Cloud Anwendungen ist für die Benutzer nicht ersichtlich, wo im Internet seine Daten liegen und wer darauf Zugriff hat, wo Berechnungen tatsächlich durchgeführt werden oder wer tatsächlich der Urheber ausgeführter Anwendungen oder von Anwendungsteilen ist. Cloud Dienste bieten daher ein breites Betätigungsfeld für Kriminelle sowohl als Ziel für schädigende Aktivitäten als auch als Tatwerkzeug, da die Verteilung auch das Sichern forensischer Spuren erschwert.

Mobil und transparent

Aktuelle mobile Endgeräte wie Tabletts und Smart-Phones sind vollwertige Computersysteme mit zum Teil offenen Betriebssystemen und einem umfangreichen Ökosystem an verfügbaren Apps. Dabei kommt diesen Geräten eine immer zentralere Rolle im täglichen Leben zu. Neben der Grundfunktion des Telefonierens übernehmen unsere mobilen Geräte immer sensiblere Aufgaben wie Tele-Banking und elektronische Zahlung wobei sensible Informationen in Form von Zugangsdaten, PINs und TANs direkt am Gerät eingegeben, oft aber sogar gespeichert werden. Aktuelle Trends zeigen, dass Kriminelle vermehrt unter Ausnutzung der Gutgläubigkeit der Anwenderinnen und Anwender, aber auch unter Nutzung komplexer Schadsoftware, Anwenderdaten ausspähen, Zugangsdaten entwenden und mißbräuchlich verwenden, und sogar betrügerische Banktransaktionen über das Endgerät des Benutzers abwickeln.

Das Phänomen Cybercrime hat verschiedenste Facetten. Die von ihr ausgehenden Gefahren sind in ihrem Ausmaß und in ihren Erscheinungsformen weiterhin bedeutsam. Nach Einschätzung des Bundeskriminalamts wird daher der Bereich Cybercrime auch in den kommenden Jahren ein wachsendes Phänomen darstellen. Dessen Bekämpfung durch die Sicherheitsbehörden wird sowohl präventiv als auch repressiv im Sinne eines ganzheitlichen Ansatzes fortgesetzt. Dabei stehen vorausschauendes Denken, die Erstellung umfassender Strategien und Kooperationen mit der Wirtschaft und Wissenschaft im Mittelpunkt.

KRIMINAL PRÄVENTION POLIZEI

IT-Sicherheit: So schützen Sie sich im Internet

Eines der größten Risiken im Netz ist ein mangelnder Schutz der Daten: Persönliche Angaben, Kreditkartennummern und Bankverbindungen können leicht in falsche Hände geraten. Mit einer gesunden Portion Vorsicht und diesem Basiswissen sind Internetnutzer indes gut gerüstet.

Sicher im Netz: 10 Tipps wie Sie sich vor Gefahren schützen können

1. Schutz des PC

An oberster Stelle steht eine gute Sicherheitsausstattung für Ihren Computer. Um den PC vor schädlichen Dateien zu schützen, sollten vor der ersten Nutzung des Internets ein Anti-Viren-Programm und eine Firewall installiert werden. Für diese Schutzprogramme, das Betriebssystem und den Internet-Browser werden regelmäßig von den Herstellern Aktualisierungen, so genannte Updates, angeboten, die auch automatisiert abgerufen werden können. Es wird empfohlen diese Updates umgehend zu installieren. Das gilt auch für auf dem PC installierte Anwendungsprogramme. Da Schadsoftware zunehmend über externe Datenträger wie CDs oder USB-Sticks verbreitet wird, sollten diese vor der Nutzung auf Viren geprüft werden.

2. E-Mails und Chat

Öffnen Sie nur E-Mails, die von vertrauenswürdigen Absendern stammen. Dubiose Mails von Unbekannten möglichst sofort löschen. Schadprogramme verbergen sich oft in Grafiken oder E-Mail-Anhängen. Verdächtige Dateien sollten Sie auf keinen Fall öffnen! Vorsicht auch vor angeblichen E-Mails von Kreditinstituten: Banken bitten Kunden nie per Mail, vertrauliche Daten im Netz einzugeben. Auch in Communitys empfangene E-Mail-Anhänge sollten mit einem Schutzprogramm überprüft werden. Riskant können auch Chat-Nachrichten von Unbekannten sein: Kriminelle versenden oft Links zu Webseiten mit Viren. Das Aufrufen dieser Seiten installiert Ihnen möglicherweise bereits eine Schadsoftware (Malware).

3. Software

Achten Sie darauf, welche Software oder Zusatzprogramme („Plug-Ins“) Sie installieren. Eine Gefahr sind Schadprogramme, die in Gratis-Downloads oder Raubkopien von dubiosen Anbietern versteckt sind. Gesundes Misstrauen hilft: Wenn Zweifel an der Seriosität bestehen, besser auf Download und Installation einer Software verzichten.

4. Tauschbörsen

Wer im Internet mit Unbekannten Dateien tauscht, riskiert eine Infektion seines PCs mit Schadprogrammen. Zudem ist der Tausch von urheberrechtlich geschützten Musik-, Film- oder Software-Kopien strafbar und kann gegebenenfalls neben Geld- und Freiheitsstrafen zu Schadenersatzansprüchen der Rechteinhaber führen.

5. Online-Shopping

Zeichen für die Seriosität eines Online-Shops sind ein Impressum mit Nennung und Anschrift der Firma, des Geschäftsführers oder einer Umsatzsteuer-Identifikationsnummer (UIDNummer) sowie klare Geschäftsbedingungen (AGB). Kunden sollten auch die Datenschutzerklärung lesen. Manche Shops werden von unabhängigen Experten geprüft und erhalten ein Zertifikat oder Siegel. Auch der Kunde kann Kontrolle ausüben: Auf vielen Shopping-, Preisvergleich- und Auktionsseiten werden Händler beurteilt. Gute Bewertungen können ein Hinweis auf seriöse Geschäftspraktiken

sein. In jedem Fall ist jedoch eine Portion gesundes Misstrauen angebracht – vor allem auf Webseiten mit Angeboten weit unter dem tatsächlichen Wert. Weiterführende Informationen sowie „nicht zu empfehlende Webseiten" bieten die verschiedenen nationalen und internationalen Konsumentenschutzorganisationen (www.europakonsument.at).

6. Bezahlung im Web

Beim Kauf von Waren im Internet ist allgemein Vorsicht geboten, insbesondere bei Vorauszahlung. Zur Bezahlung sollten Konto- oder Kreditkartendaten über eine verschlüsselte Verbindung übertragen werden, erkennbar an den Buchstaben „https" in der Adresszeile der Webseite und einem Schloss- oder Schlüssel-Symbol im Internet-Browser. Sichere Webseiten sind auch an einer grün hinterlegten Adresszeile oder an einem grün hinterlegten Zertifikatszeichen erkennbar, wenn sich der Betreiber einer unabhängigen Prüfung unterzogen hat. Zahlungen können per Lastschrift, Kreditkarte oder Rechnung erfolgen. Es gibt auch seriöse Bezahl-Dienste, bei denen die Bankdaten einmalig hinterlegt werden. Vorkasse per Überweisung ist zwar weit verbreitet, gilt aber generell als sehr viel riskanter.

7. Online-Banking

Beim Online-Banking sollte man die offizielle Adresse der Bank immer direkt eingeben oder über eigene Lesezeichen, so genannte Favoriten, aufrufen. Maßgeblich ist die Adresse, die die Bank in ihren offiziellen Unterlagen angibt. Die Verbindung zum Bankcomputer muss wie bei Bezahlvorgängen verschlüsselt sein (erkennbar an den Buchstaben „https" in der Adresse der Webseite). Für Überweisungen und andere Kundenaufträge sind Transaktionsnummern (TANs) nötig. In den Anfängen des Online-Bankings konnten die Nutzer einen solchen Code aus einer Liste frei wählen. Sicherer ist das iTAN-Verfahren, bei dem die Codes nummeriert sind. Ein Zufallsgenerator der Bank bestimmt, welche TAN eingegeben werden muss. Noch weniger Chancen haben Kriminelle beim mTAN-Verfahren: Die TAN wird dem Kunden aufs Handy geschickt und ist nur kurzzeitig gültig. Weitere Schutzverfahren sind eTAN und HBCI, bei denen der Kunde als Zusatzgeräte einen TANGenerator oder ein Kartenlesegerät nutzt. PC-Nutzer sollten Ihre Bank fragen und das modernste verfügbare Verfahren wählen.

Vorsicht gilt, falls mehrere Transaktionsnummern auf einmal abgefragt werden: Dann ist Phishing im Spiel. Phishing ist eine Art von Diebstahl persönlicher Daten über das Internet. Über E-Mails oder betrügerische Webseiten wird versucht, persönliche Daten oder Informationen wie Kreditkartennummern, Kennwörter, Kontodaten usw. abzufragen. In diesem Fall informieren Sie bitte sofort Ihr Bankinstitut.

8. Private Infos und Passwörter

Die meisten Menschen würden im Alltag kaum Unbekannten ihr Privatleben offenbaren. Auch im Web haben es die Nutzer in der Hand, den Zugang zu privaten Infos zu beschränken. Nur gute Bekannte sollten in entsprechenden Foren und Communitys Zugriff auf Fotos oder Kontaktdaten erhalten. Je weniger von der eigenen Privatsphäre frei zugänglich ist, desto weniger Angriffsfläche wird potenziellen Tätern und anderen unbefugten Nutzern geboten. Seien Sie bei der Weitergabe Ihrer E-Mailadresse oder bei der Eintragung Ihrer Daten in Internetformulare vorsichtig. Gehen Sie immer davon aus, dass Ihre Daten weitergegeben und missbraucht werden können.

Bei vielen Online-Services müssen sich die Nutzer registrieren. Meist werden Benutzername und Passwort festgelegt. Soweit möglich, verwenden Sie nicht das gleiche Passwort für mehrere Dienste – etwa E-Mail-Konto, Online-Shops und Communitys. Je länger ein Passwort, desto schwerer ist es zu knacken. Es sollte mindestens acht Zeichen lang sein und aus einer zufälligen Reihenfolge von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Ein solches könnte leicht erstellt werden, indem sich der Benutzer einen Satz überlegt und von jedem Wort den ersten Buchstaben sowie alle Zahlen und Sonderzeichen verwendet. (zum Beispiel der Satz: „Ich bin am 1. Jänner 1970 geboren." ergäbe das Passwort: Iba1.J1970g.)

Wer sich die zahlreichen Codes schwer merken kann, dem helfen so genannte Passwort-Safes. Das sind PC-Programme, mit denen sich Geheimzahlen sicher speichern lassen. Der Anwender braucht sich dann nur noch ein Haupt-Passwort zu merken.
Speichern Sie weiters keine Passwörter (PIN, TAN...) auf dem PC. Mitarbeiter von Banken werden Sie nie nach Zugangsdaten fragen. Anfragen per Mail kommen in der Regel ausschließlich von Betrügern.

9. Angebote als Waren- oder Finanzagenten

Angebote im Internet oder per E-Mail als Waren- oder Geldvermittler zu arbeiten, sind konsequent abzulehnen. Der Vermittler dient den Tätern zur Verschleierung ihrer Identität. Web-Nutzer, die sich auf dubiose Angebote einlassen und Waren oder Gelder weiterleiten, betreiben Beihilfe zum Betrug oder der Geldwäsche und müssen mit strafrechtlichen Folgen und Schadenersatzansprüchen rechnen.

10. Apps und Abofallen

Seien Sie sich bewusst, dass Apps Kosten verursachen sowie sensible Nutzerdaten übertragen können. Dies kann oftmals passieren ohne dass diese für die Funktion der Apps notwendig sind. Installieren Sie daher nur Apps über die offiziellen App-Shops, da diese überprüft bzw. bei Problemen mittels Fernlöschung von Ihrem Handy entfernt werden. Seien Sie besonders bei kostenlosen Apps vorsichtig. Achtung geboten ist zudem bei Online-Diensten bei denen eine Registrierung erforderlich ist. Neben der breiten Masse der seriösen Werbeangebote gibt es auch Fallen, bei denen versteckt Bestellungen oder Abo-Verträge abgeschlossen werden. Die Nutzer werden dabei nicht ausreichend über die Vertragsbedingungen und Preise informiert. Oft wird dies erst im Nachhinein bemerkt, wenn Rechnungen bzw. Inkassoschreiben eingehen. Hilfestellung hierbei bietet die Watchlist des Internetombudsmannes, der auch als außergerichtliche Schlichtungsstelle in Streitfragen fungiert. Im Internet zu finden unter www.ombudsmann.at

Sicherheit und Datenschutz bei Handys

Die Mobilfunkbranche ist ein Bereich, der durch schnelle Entwicklungen geprägt ist und in dem die Technik mit atemberaubender Geschwindigkeit voranschreitet. In nur wenigen Jahren haben wir eine Entwicklung vom Mobiltelefon mit einfachen Fähigkeiten - wie der Möglichkeit, Telefonanrufe zu tätigen und Textmitteilungen (SMS) zu versenden – zu einer viel komplexeren Technik mitgemacht, die den Handynutzern eine breitere Palette an Diensten eröffnet. Neue Geräte (iPhones, Smartphones, etc.) bieten zunehmend mehr Funktionalitäten wie Internetzugang, E-Mail, WLan, MMS - Multimediamitteilungen , Videokonferenz, GPS (Navi) u.v.m.

Sobald sich ein Mobiltelefon im Besitz einer Person befindet, wird es ein wichtiger (personalisierter) Bestandteil im Berufs- und Privatleben. Es enthält sehr sensible (persönliche, dienstliche oder geschäftliche) Informationen, welche für „Datensammler" oder Straftäter zunehmend interessanter werden. Also jene Informationen, welche vom Telefon (zumeist unbemerkt) übermittelt werden und Dritten die Möglichkeit bieten, den Standort zu bestimmen oder sich generell Zugang zum Gerät und den darauf gespeicherten Daten zu verschaffen. Weitere Angriffspunkte stellen WLAN und Bluetooth dar. Ein Angreifer kann über diese Funkschnittstellen das Betriebssystem und alle Dienste des Gerätes beliebig manipulieren und das betroffene Handy für „seine" Zwecke konfigurieren.
Bei der Nutzung von internetfähigen Smartphones ist die Sicherheit und der Schutz der gespeicherten Daten genauso wichtig wie bei jedem anderen Computer auch.

Besondere Vorsicht ist daher auch bei der Installation und Verwendung von Apps geboten. So hilfreich und unterhaltsam diese Mini-Anwendungen auch sein mögen, bergen sie aber gleichsam die Gefahr in sich, dass vertrauliche Daten wie z.B. GPS-Koordinaten, SMS, Kontaktdaten und Telefonnummern (für den Besitzer unbemerkt) an Werbefirmen oder Softwareentwickler übermittelt und missbräuchlich verwendet werden. Fast die Hälfte der Android-Apps enthalten Programmcodes, welche für Werbezwecke oder zur Analyse des Nutzungsverhaltens eingesetzt werden können. Beim iPhone liegt die Anzahl derzeit bei ca. 25%.
Zum Schutz der Handydaten sollten folgende Punkte berücksichtigt werden:

1. Verwendung von PIN und persönlichen Telefon(sicherheits)codes
2. WLAN und Bluetooth-Funktion nur aktiveren, wenn diese benötigt werden
3. Das Handy nie unbeaufsichtigt lassen oder fremden Personen anvertrauen
4. Vertrauliche Daten der Speicherkarte gegebenenfalls verschlüsseln
5. Nur Apps aus sicheren Quellen beziehen, im Zweifelsfall nicht installieren
6. Nicht benötigte Zusatzdienste oder Zusatzfunktionen (z.B. GPS) deaktivieren
7. Vorsicht bei SMS (MMS), welche von einer unbekannten Rufnummer stammen, besonders wenn diese einen Link enthalten, zum Download einer Datei auffordern bzw. die Installation von Anwendungen „anregen"

Da der Verlust oder Diebstahl des eigenen Handys nie ausgeschlossen werden kann empfiehlt sich auch eine regelmäßige Sicherung der gespeicherten Daten (Kontakte, Notizen, etc.). Weiters sollte man PIN, PUK, Rufnummer, SIM-Kartennummer und Seriennummer des Telefons (IMEI) sicher aufbewahren, da diese Daten für die Sperre der SIM-Karte beim Mobilfunkbetreiber und für die Anzeigeerstattung (Verlust, Diebstahl) erforderlich sind. Die IMEI befindet sich bei den meisten Geräten unter dem Akku und zusätzlich auf der Originalverpackung. Beim eingeschalteten Handy kann die IMEI mittels *#06# abgerufen werden.

Sicherheitstipps für Unternehmen

1. Schulung und Sensibilisierung
Zur Vorbeugung von Bedrohungen und zur Reduzierung von Risiken leistet das Mittel der Mitarbeiterschulung den größten und wirkungsvollsten Beitrag. Aufmerksamkeit und kritisches Hinterfragen im Tagesgeschäft ist ebenfalls von äußerster Bedeutung. Gegenseitige Kontrolle besonders bei sicherheitsrelevanten Handlungen kann Fehler aufzeigen und abwenden.

2. Zugriffsschutz
Passwörter sollten nicht notiert und stets geheim gehalten werden, sowie einer zuvor festgelegten Richtlinie entsprechen. Ein gutes Passwort besteht in der Regel aus mindestens 8 Zeichen, wobei diese Zeichenfolge aus Zahlen, Buchstaben und Sonderzeichen bestehen muss um einfachen Wörterbuchattacken standhalten zu können. Regelmäßiges Ändern eines Passworts hebt das Sicherheitsniveau zusätzlich. Geräte denen durch einen Hersteller ein Standard-Passwort vergeben wurde, sind mit einem neuen Passwort zu versehen, da diese durch den Hersteller vorgegebenen Passwörter meist öffentlich bekannt sind.

3. Wireless LAN (WLAN)
In den Einstellungen eines WLAN-Routers ist es notwendig den Verschlüsselungsstandard WPA oder WPA-2 zu wählen. Sollte das Gerät nicht über eine dieser Einstellungen verfügen ist wenigstens der unsichere Standard WEP zu verwenden. Bei der Konfiguration eines WLANs ist darauf zu achten, dass Standard-Schlüssel die durch den Hersteller vorgegeben wurden, durch einen eigenen geheimen Schlüssel ersetzt werden. Die Bezeichnung der sogenannten SSID ist neutral zu vergeben, damit von außerhalb das Drahtlosnetzwerk einer bestimmten Einrichtung nicht zugeordnet werden kann.

4. Sicherheitssoftware
Anti-Viren Programme und Firewalls können einen Computer bzw. ein Netzwerk nur dann schützen, wenn diese Programme durch regelmäßige Updates gepflegt werden. Dies betrifft grundsätzlich auch alle anderen Programme die auf einem Computer installiert wurden, damit bekannte Sicherheitslücken geschlossen werden können.

5. Schutz sensibler Daten
Auf externen Datenträgern (USB-Sticks, externen Festplatten, DVDs usw.) dürfen keine Daten unverschlüsselt gespeichert werden, die nicht für die Öffentlichkeit bestimmt sind. Beim Verlassen des Arbeitsbereichs kann durch gleichzeitiges Betätigen der Tasten „Windows-Taste+L“ ein Computer mit Windows-Betriebssystem gesperrt werden, Papierdokumente und Datenträger sind bei längerer Abwesenheit vom Arbeitsbereich ebenfalls zu entfernen.

6. Sichere Webseiten
Die Preisgabe von internen Informationen auf Webportalen oder Informationen durch aussagekräftige Fehlermeldungen auf Webseiten im Falle eines Systemfehlers verschaffen Angreifern wesentliche Vorteile. Versionsnummern von Softwareprodukten, der Herstellername der Software, sowie aussagekräftige Fehlermeldungen (Angabe der fehlerhaften Datei oder des Speicherorts der Datei) sind Informationen, die es zu schützen gilt. Alle vertraulichen Informationen auf Webservern sind in ein passwortgeschütztes Verzeichnis abzulegen. Damit bestimmte Verzeichnisse bzw. Passwortdateien nicht durch eine Suchmaschine gefunden werden können, kann eine „robots.txt“ im Stammverzeichnis des Webservers verwendet werden. Falls

kein Zugriff zum Stammverzeichnis erfolgen kann, sind „Meta-Tags“ (<meta name=“robots“ content=“noindex“>) im „Header“ der Webseite hilfreich.

7. Social Engineering

Der erste Schritt eines Hackers beginnt mit dem Ausforschen von Informationen. Diese Informationen erlangen Angreifer meist durch Anrufe mit gefälschter Identität oder durch die persönliche Begehung des Geschäftsbereichs. Nützliche Informationen befinden sich oftmals in Mülltonnen in denen (DVDs, CDs, Post-its) oder Ausdrucke firmeninterner Informationen vollständig enthalten sind. Papierdokumente oder Datenträger sind daher vor der Entsorgung fachgerecht durch entsprechende mechanische Verfahren zu vernichten.

Sicher vor Betrügereien im Netz

3,1 Millionen Österreicherinnen und Österreich sind Onlin-Shoper. Der Marktplatz Internet wird aber auch von Internetbetrügern missbraucht. Dazu werden Internetseiten von namhaften Markenherstellern gefakt und Modeartikel, Parfüms, Computer- oder Elektrogeräte zu besonders günstigen Preisen zum Kauf angeboten. Die Opfer werden zur Vorauskasse aufgefordert – die Ware bzw. ihr bezahltes Geld sehen sie aber nie.

Tipps des Bundeskriminalamts

Seien Sie bei der Jagd nach sogenannten Internet-Schnäppchen besonders vorsichtig. Mit einem vermeintlich „günstigem" Angebot können Sie sehr schnell in eine Internetfalle tappen. Das Bundeskriminalamt warnt daher vor dubiosen Einkäufen im Internet und gibt folgende Tipps:

- Zunächst gilt natürlich, dass bekannte, etablierte Unternehmen auch online ähnlich seriös agieren wie in der „realen" Welt. Zeichen für die Seriosität eines Online-Shops sind ein Impressum mit Nennung und Anschrift der Firma, des Geschäftsführers oder einer Umsatzsteuer Identifikationsnummer (UID-Nummer) sowie klare Geschäftsbedingungen (AGB).

- Weiters sollten leicht zugängliche und transparente Vertragsbedingungen für den Online-Einkauf bereitgestellt als auch die Leistungsmerkmale der angebotenen Produkte und die Garantiebedingungen genau und übersichtlich online abrufbar sein.

- Kunden sollten auch die Datenschutzerklärung lesen.

- Manche Shops werden von unabhängigen Experten geprüft und erhalten ein Zertifikat oder Siegel (www.europakonsument.at).

- Auch der Kunde kann Kontrolle ausüben: Auf vielen Shopping-, Preisvergleich- und Auktionsseiten werden Händler beurteilt. Gute Bewertungen können ein Hinweis auf seriöse Geschäftspraktiken sein.

- Ein wichtiges Kriterium ist auch das Österreichische E-Commerce-Gütezeichen. Shops, die mit dem E-Commerce Gütezeichen zertifiziert sind, können Sie aufgrund der strengen Prüfkriterien vertrauen. Informationen dazu finden Sie auf www.guetezeichen.at.

Bezahlung im Web

Beim Kauf von Waren im Internet ist allgemein Vorsicht geboten, insbesondere bei Vorauszahlung. Wählen Sie daher alternative Bezahlsysteme und sehen sie zusätzlichen Kosten für eine Nachnahmesendung als eine Art Versicherung an. Zur Bezahlung sollten Konto- oder Kreditkartendaten über eine verschlüsselte Verbindung übertragen werden, erkennbar an den Buchstaben „https" in der Adresszeile der Webseite und einem Schloss- oder Schlüssel-Symbol im Internet-Browser. Sichere Webseiten sind auch an einer grün hinterlegten Adresszeile oder an einem grün hinterlegten Zertifikatszeichen erkennbar, wenn sich der Betreiber einer unabhängigen Prüfung unterzogen hat. Zahlungen können per Lastschrift, Kreditkarte oder Rechnung erfolgen. Es gibt auch seriöse Bezahl-Dienste, bei denen die Bankdaten einmalig hinterlegt werden. Vorkasse per Überweisung ist zwar weit verbreitet, gilt aber generell als sehr viel riskanter. Eine gute Alternative zur Zahlung mit Kreditkarte ist die Lieferung per Nachnahme. Die ist zwar meist etwas teurer, aber dafür sehr sicher, da Sie erst bezahlen, wenn Sie das Paket schon in Händen halten.

Schutz vor Phishing

Was ist Phishing?

Phishing ist ein Versuch persönliche Daten über das Internet zu erlangen. Über E-Mails und betrügerische Webseiten wird versucht, persönliche Daten oder Informationen wie Kreditkartennummern, Kennwörter, Kontodaten usw. abzufragen. Phishing gibt es in unterschiedlichsten Varianten. Fingierte E-Mails etwa sollen beim Nutzer den Eindruck erwecken, sie kämen von seiner Bank oder einem Online-Auktionshaus. Die Empfängerin oder der Empfänger wird aufgefordert, einen Link anzuklicken - vom dem er zu einer meist täuschend echt aussehenden Betrugs-Webseite geleitet wird. Dort wird der Nutzer unter einem Vorwand gebeten, seine persönlichen Daten – darunter auch Passwörter – einzutragen. Bei Verdachtsmomenten kontaktieren Sie bitte sofort Ihr Bankinstitut!

Tipps des Bundeskriminalamts

- Kein seriöses Unternehmen oder Bankinstitut fordert per E-Mail zur Eingabe von persönlichen Daten wie Passwörter usw. auf.

- Internetseiten, auf denen man sensible Nutzerdaten eingeben muss, erkennen Sie an den Buchstaben „https“ in der Adresszeile der Webseite und einem Schloss- oder Schlüssel-Symbol im Internet-Browser. Weiters sind sichere Webseiten auch an einer grün hinterlegten Adresszeile oder an einem grün hinterlegten Zertifikatszeichen erkennbar, wenn sich der Betreiber einer unabhängigen Prüfung unterzogen hat.

- Überprüfen Sie die Adressezeile des Webbrowsers. Oft reicht ein Blick, um zu erkennen, dass es sich gar nicht um die richtige Website handelt.

- Richten Sie sich Ihre wichtigen Homepages, wie zum Beispiel Bankzugang etc. als Favoriten in Ihrem Browser ein und verwenden Sie nur diese. Stellen Sie so sicher, dass Sie nur die offiziellen Seiten verwenden.

- Wichtig ist der Schutz durch Passwörter: Soweit möglich, verwenden Sie nicht das gleiche Passwort für mehrere Dienste – etwa E-Mail-Konto, Online-Shops und Communitys. Je länger ein Passwort, desto schwerer ist es zu knacken. Es sollte mindestens acht Zeichen lang sein und aus einer zufälligen Reihenfolge von Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen bestehen. Ein solches könnte leicht erstellt werden, indem sich der Benutzer einen Satz überlegt und von jedem Wort den ersten Buchstaben sowie alle Zahlen und Sonderzeichen verwendet (zum Beispiel der Satz: „Ich bin am 1. Jänner 1970 geboren.“ ergäbe das Passwort: Iba1.J1970g.) Wer sich die zahlreichen Codes schwer merken kann, dem helfen so genannte Passwort-Safes. Das sind PC-Programme, mit denen sich Geheimzahlen sicher speichern lassen. Der Anwender braucht sich dann nur noch ein Haupt-Passwort zu merken.

- Sind Sie sich unsicher, ob Sie ein Passwort bekannt gegeben haben, dann ändern Sie als erstes das Passwort und melden Sie diesen Vorgang an die Betreiber der Homepage bzw. dem Unternehmen.

Sicherheit im Social Network

Beim Thema Internet kennen sich Jugendliche häufig besser aus als ihre Eltern. Das heißt aber nicht, dass sie auch sicher im Netz unterwegs sind und immer wissen, wie sie sich verhalten sollen. Worauf Kinder und Eltern achten sollten. Für Jugendliche und ihr soziales Leben sind Internet und Netzwerkplattformen unentbehrlich geworden. Das bestätigt auch eine aktuelle internationale Studie über die Onlinenutzung von Kindern und Jugendlichen: 98 Prozent der neun- bis 16jährigen Kinder in Österreich nutzen das Internet zuhause, 48 Prozent im eigenen Kinderzimmer. 62 Prozent haben ein eigenes Profil innerhalb eines sozialen Netzwerks, wie zum Beispiel Facebook. Rund die Hälfte der Kinder haben 50, ein Viertel mehr als 100 Freunde im Netz. 20 Prozent der Kinder, die ein Profil haben, geben an, dieses sei öffentlich einsehbar, 15 Prozent geben persönliche Daten, wie Telefonnummer und Adresse bekannt. Immer mehr Kinder nutzen soziale Netze, aber viele vernachlässigen ihre Sicherheit im Internet. Oft geben Kinder aus Unwissenheit private Daten und Informationen weiter. Dabei setzen sie sich aber großen Gefahren aus und sind leichte Beute für Online-Belästigungen oder Cyber-Mobbing. Dem eigenen Kind das Mitmachen zu verbieten, wenn alle Freunde in sozialen Netzwerken unterwegs sind, ist keine Lösung und es ist auch schwer kontrollierbar. Wie in vielen anderen Bereichen ist Reden und Aufklären die wesentlich bessere Alternative.

Wer garantiert für Sicherheit?

„Wie sicher sind soziale Netzwerke? Und sollte ich meinem Kind Facebook erlauben?“ Diese oder ähnliche Fragen werden häufig von Eltern gestellt. Leider gibt es auf diese Frage keine einfache Antwort. Ob ein Kind für soziale Netzwerke „bereit“ ist, hängt von seinem Grad der Reife ab – und davon, wie die Eltern ihre Kinder auf die Welt der sozialen Netzwerke vorbereitet haben. Fest steht: soziale Netzwerke sind nur für Kinder ab 13 Jahre. Was nicht bedeutet, dass es nicht genutzt wird. Denn viele Jugendliche besuchen die sozialen Netzwerke ihrer älteren Freunde oder Geschwister oder geben ein falsches Alter an – einfach, um dabei zu sein. Wichtig ist es, die Kinder über soziale Netzwerke zu informieren bzw. sie darauf vorbereiten. Hier einige Tipps zum sicheren Umgang mit sozialen Netzwerken.

Tipps und Empfehlungen für Eltern

- Sicherheitsregeln vermitteln: Kinder und Jugendliche sollen darauf vorbereitet werden, dass der Gesprächspartner im Internet oft nicht der ist, für den er sich ausgibt. Sie sollen daher auch niemanden als Freund akzeptieren, den sie in der realen Welt nicht kennen. Weiters sollen keine Fotos und andere Dokumente im Sozialen Netzwerk veröffentlicht werden, die sie möglicherweise später bereuen werden. So sollen auch Kenn- oder Passwörter in Netzwerken nicht weitergegeben werden, auch nicht an Freunde. Das gilt auch für persönliche Informationen, wie Anschrift, Telefonnummer oder Urlaubspläne.

- Wissen was ihr Kind tut: Eltern sollten die sozialen Netzwerke und Chat-Räume, in denen sich Kinder und Jugendliche bewegen, kennen. Zeigen Sie Interesse an ihren Chat-Aktivitäten, daran, was sie fasziniert, und mit wem sie sich unterhalten. Vereinbarungen treffen: Online in einem Profil auf einem sozialen Netzwerk zu sein, ist eine Form von Medienkonsum. Eltern sollten mit ihren Kindern altersgemäße Vereinbarungen treffen, wie lange sie wo und mit wem chatten dürfen. Die Zeit in Netzwerken darf Freundschaften im realen Leben nicht verdrängen oder ersetzen.

- Anlaufstelle bieten: Kinder sollten jederzeit zu ihren Eltern, Freunden oder Bekannten kommen können, wenn sie Fragen haben oder online etwas passiert, das ihnen ein ungutes Gefühl gibt. Werden Sie selbst Mitglied im Netzwerk: Selbst wenn sie soziale Netzwerke nicht als soziales Medium nutzen möchten, sollten Sie sich registrieren und ein „Freund" Ihres Kindes werden. Dann müssen Sie sich nicht auf seiner Webseite einloggen, um zu sehen , was es veröffentlicht. Ihr Kind möchte nicht, dass Sie in seiner Freundesliste erscheinen? Schlagen Sie ihm vor, dass Sie sich eine Identität zulegen, aus der nicht sofort hervorgeht, dass Sie ein Elternteil sind. Auf diese Weise weiß Ihr Kind, dass Sie da sind – seine Freunde müssen dies jedoch nicht unbedingt erfahren.

Soziale Netzwerke sollten weder verteufelt werden noch ist es notwendigerweise für Ihr Kind schädlich. Es kann Ihrem Kind sogar helfen, Freundschaften zu pflegen, mit Verwandten in Kontakt zu bleiben und das, was ihm wichtig ist, mit Freunden und Familienmitgliedern zu teilen. Wie bei allen anderen Dingen im Leben kommt es auch hier auf das richtige Maß an. Die Aufgabe der Eltern ist es, dafür zu sorgen, dass es diese sozialen Netzwerke sicher nutzen kann.

Tipps und Empfehlungen für Kinder und Jugendliche

- Schütze deine Privatsphäre: Achte darauf, welche Informationen du über dich ins Internet stellst. Poste keine Bilder oder Texte, die später einmal gegen dich verwendet werden könnten. Veröffentliche keine persönlichen Daten wie Name, Adresse, Handynummer, Passwörter etc. Verwende die Einstellungen zur „Privatsphäre", damit Fremde nichts über dich erfahren können.

- Sei misstrauisch: Viele Behauptungen die auf sozialen Plattformen gepostet werden sind nicht wahr. Oft ist nicht klar, woher die Infos stammen. Man weiß nie, ob jemand wirklich der ist, der er oder sie vorgibt zu sein. Überprüfe Infos aus dem Internet daher mehrfach!

- Urheberrechte beachten: Das Anbieten und Weiterverwenden (z.B. in Blogs, Profilen) von Musik, Videos, Bildern und Software ist – ohne Einwilligung der Urheber/innen – verboten. Mehrere Tausend Euro Strafe können die Folge sein. Eine Ausnahme sind Werke, die unter einer Creative Commons-Lizenz stehen. Wenn du Textteile anderer Autor/innen verwendest, führe immer eine Quellenangabe an.

- Das Recht am eigenen Bild: Es ist nicht erlaubt Fotos oder Videos, die andere zu ihren Nachteil darstellen, zu veröffentlichen. Frag zur Sicherheit die betroffenen Personen vorher, ob sie mit der Veröffentlichung einverstanden sind.

- Vorsicht bei gratis-Angeboten: Kostenlos ist selten etwas. Sei besonders misstrauisch, wenn du dich mit Namen und Adresse registrieren musst.

- Hol dir Rat bei Erwachsenen: Wenn dir etwas merkwürdig vorkommt, dann sprich darüber mit Erwachsenen, denen du vertraust. Auf merkwürdige oder bedrohliche Nachrichten nicht antworten.

Schutz vor Grooming

Was ist Grooming?

Bei Grooming handelt es sich um das gezielte Ansprechen von unmündigen, unter 14-jährigen Kindern mit dem Ziel der Anbahnung sexueller Kontakte. Es stellt demnach eine besondere Form der sexuellen Belästigung dar. Bis zur Strafgesetznovelle 2011, die mit 1. Januar 2012 in Kraft trat, gab es in Österreich gegen Grooming keine gesetzliche Handhabe. Der neu geschaffene § 208a Strafgesetzbuch schafft nun Abhilfe und stellt Grooming sowohl im Wege der Telekommunikation als auch im virtuellen und im realen Raum unter Strafe.

Tipps „Cyber-Grooming"

Kinder und Jugendliche fühlen sich in Chaträumen im Internet oft anonym und sicher. Doch immer öfter werden sie Opfer des „Cyber Groomings", der gezielten Anmache im Netz. Die Täter sind meist ältere Männer, die sich in der virtuellen Welt das Vertrauen ihrer jungen Opfer erschleichen. Nicht selten mit dem Ziel, sich auch im realen Leben mit ihnen zu treffen und sie zu missbrauchen.

Das Bundeskriminalamt gibt folgende Tipps

- Kinder und Jugendliche sollten darauf vorbereitet werden, dass der Gesprächspartner im Internet oft nicht der ist, für den er sich ausgibt. Erklären Sie ihnen, dass sie diesen Umstand in Chaträumen als auch in den sozialen Netzwerken stets bedenken sollten
- Erklären Sie Ihrem Kind, welche Medieninhalte genutzt werden dürfen und welche nicht. Machen Sie Ihre eigenen Standpunkte deutlich
- Sprechen Sie mit Ihrem Kind über sein Verhalten im Internet. Was gefällt ihm? Was erlebt er oder sie? In welchen Chatrooms bewegen sie sich? Wo liegen mögliche Gefahren?
- Machen Sie sich kundig über die Technik und Umgangsweise in Chaträumen, damit Sie mitreden und Fragen stellen können. Auf diese Weise gelten Sie für ihre Kinder viel eher als Ansprechperson um über belastende Erfahrungen im Internet zu reden
- Diskutieren Sie darüber, welche Bilder ins Netz gestellt werden. Denken Sie daran, dass auf die Gefühle des Betrachters keine Einflussmöglichkeit besteht!
- Überprüfen Sie die Sicherheitseinstellungen Ihres Computers. Es gilt allerdings zu bedenken, dass auch Filterprogramme für den Computer nicht immer wirkungsvoll sind
- Üben Sie mit Ihrem Kind konkrete Möglichkeiten, wie es sich vor sexueller Belästigung und Missbrauch im Netz schützen kann. Verbale sexuelle Belästigung können Kinder und Jugendliche manchmal schon mit einem klaren Nein beenden
- Mädchen und Burschen sollten wissen, welches Verhalten das Risiko einer sexuellen Ausbeutung erhöhen und was sie auf jeden Fall unterlassen sollten: wie etwa Informationen über die eigene Identität zu geben, Fragebogen im Netz auszufüllen und sich mit nicht persönlich bekannten Chatfreunden ohne Begleitung von Erwachsenen zu treffen

Glossar: Computerlatein

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

Backdoor ist eine verbreitete Schadfunktion welche 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 Unter einem BotNet oder Bot-Netz (die Kurzform von Roboter Netzwerk) versteht man ein fernsteuerbares Netzwerk (im Internet) von Computersystemen, welches 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.

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

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

C&C–Server Command and Control Server zumeist übernommene oder unter falscher Identität angemietete Rechner zur Steuerung der Bots.

Computervirus Ein Computervirus ist 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 ähnelt einem Computervirus, verbreitet sich aber direkt über Netzwerke wie dem Internet und versucht in andere Computer einzudringen. Es 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.

Darknet bezeichnet eine Sammlung von Verfahren und Technologien die eine anonymen Datenaustausch und Kommunikation im Internet ermöglichen. Es wird auch als Untergrund Internet bezeichnet und findet unteranderem Verwendung für die Verbreitung von Illegalen Inhalten.

Deep Web bezeichnet im Allgemeinen jenen Bereich des Web der nur schwer bzw. nicht über Suchmaschinen erreichbar ist. In Verbindung mit Kriminalität können hier aber auch spezielle Umschlagplätze und geheime Netzwerke („Undernet") gemeint sein. Auf diesen wird alles Gehandelt das Spektrum reicht vom Drogen- und Waffenhandel, Dokumentenfälschung, Geldfälschung, Identitätsdiebstahl, Kinderpornografie bis zum Auftragskiller.

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

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

DoS/DDoS-Attacke Engl. Abk. „Denial of Service" = außer Betrieb setzen. 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. DDoS: Der zur Blockade führende Angriff wird nicht nur von einem einzelnen Rechner ausgeführt, sondern von mehreren gleichzeitig. Dadurch wird sowohl der Angriff verstärkt als auch die Einleitung der Gegenmaßnahmen erschwert, da diese auf mehrere Quellen angewendet werden müssen.

Drive-by-Download Darunter versteht sich ein unbeabsichtigter/unbemerkter Download von Schadsoftware während des Betrachtens (Drive-by: also im Vorbeifahren) einer Webseite. Realisiert werden derartige Drive-by-Downloads meist über eigens dafür präparierte Webseiten.

Exploit: (Zero-Day-Exploit) Ein Exploit (englisch to exploit - ausnutzen) ist eine Software oder eine Sequenz von Befehlen, welches spezifische Schwächen beziehungsweise Fehlfunktionen eines anderen Computerprogramms ausnutzt. 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 Patchs zu schließen.

Firewall (von engl. „die Brandwand") ist eine Netzwerksicherheitskomponente, die Datenverbindungen anhand eines definierten Regelwerks erlaubt oder verbietet. Das Ziel einer Firewall 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 so genannten SIM (Subscriber Identity Module), gespeichert. Die IMSI-Nummer wird weltweit einmalig pro SIM-Karte von den Mobilfunknetzbetreibern vergeben. Dabei hat die IMSI normalerweise nichts mit der Telefonnummer der SIM-Karte zu tun. Die IMSI hat immer 15 Zeichen.

Inhaltsdaten sind die Inhalte übertragener Nachrichten.

IP-Adresse Eine IP-Adresse (Internet-Protocol-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 in dem IP-Adressen verwendet werden, ist das Internet. Allen am Internet teilnehmenden Rechnern wird eine IP-Adresse zugeteilt. Die IP-Adresse entspricht funktional der Rufnummer in einem Telefonnetz.

Malware (engl. Malicious »boshaft« und Software) bezeichnet man Computerprogramme, welche vom Benutzer unerwünschte (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 – Nahfeldkommunikation
Ist ein drahtloser Übertragungsstandard. Neben dem Einsatz als Alternative zum QR-Code, bietet 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 (engl. fishing = abfischen) ist eine 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 (engl. phone freak = Telefonfreak) 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.

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 Quickresponse 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 manuell 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 Der Wortlaut Ransom stammt aus dem Englischen und bedeutet übersetzt „sich freikaufen“. Als Ransomware kann daher Schadsoftware bezeichnet werden bei der sich das Opfer durch Überweisung eines Geldbetrags praktisch freikaufen kann. Der Freikauf ist in diesem Zusammenhang mit dem Entfernen einer Sperre oder einer Entschlüsselung von Dateien eines von Ransomware betroffenen Computers zu sehen.

Server Der Begriff Server (engl. to serve = bedienen) bezeichnet entweder eine Software im Rahmen des Client-Server-Konzepts oder eine Hardware (Computer), auf der diese Software (Programm) im Rahmen dieses Konzepts abläuft.

Skriptkiddie (von „Skript“ und „Kid“) ist jemand, der leicht bedienbare, vorgefertigte Programme benutzt, um unerlaubt in fremde Computer- und Netzwerksysteme einzudringen oder durch absichtlich verbreitete Viren, Würmer oder Trojaner Schaden anzurichten. Die Bezeichnung hat Anklänge von unreifem Verhalten und Vandalismus.

Spam Unerwünschte, in der Regel auf elektronischem Weg übertragene Nachrichten, die dem Empfänger unverlangt zugestellt werden und massenhaft versandt wurden oder werbenden Inhalt haben. Dieser Vorgang wird Spamming oder Spammen genannt, der Täter Spammer.

Spyware Damit bezeichnet man 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.

TAN (M-Tan, E-TAN, I-TAN) Eine Transaktionsnummer (TAN) ist ein Einmalpasswort das im Online-Banking verwendet wird.

- M(obiler) -TAN besteht in der Einbindung des Übertragungskanals SMS.

- E-TAN ist ein kleines elektronisches Kontrollgerät, dass die (TAN) Eingabe ersetzt. Während der Kunde bisher eine Liste mit Transaktionsnummern hatte, werden über eTAN 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 eTAN-Box eingibt. Die eTAN-Box erstellt darauf eine Antwort-Nummer, mit der der Kunde die Transaktion durchführen kann.

- I-TAN oder indizierter TAN: der Kunde wird hier von der Bank aufgefordert eine bestimmte, durch eine Positionsnummer (Index) gekennzeichnete TAN aus seiner Liste einzugeben.

Trojaner (Trojanisches Pferd) ist eine 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 bezeichnet einen Vorgang, bei dem ein Klartext durch einen Verschlüsselungsalgorithmus und in der Regel geheimen Schlüssel in einen verschlüsselten Text umgewandelt wird. Man unterscheidet grundsätzlich zwischen:

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

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

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

Würmer siehe Computerwurm.

Zombie Beschreibt ein infiziertes Computersystem, das einen Teil eines BotNet bildet und durch C&C-Server kontrolliert wird.

Zugangsdaten sind jene 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: Anmerkungen

Hier geht´s zur Polizei-App