.BK

BUNDESKRIMINALAMT

# Der Cybercrime-Report: 2011

**Impressum:**
**Herausgeber:** Bundeskriminalamt, Josef-Holaubek-Platz 1, 1090 Wien;
**Fotos und Grafiken:** © Bundesministerium für Inneres (BM.I), © Bundeskriminalamt (.BK), © Interpol, © Wirtschaftskammer Österreich (WKO), © zhangsan – fotolia.com, © sinuswelle – fotolia.com, © iofoto – fotolia.com, © Nmedia – fotolia.com, © pn_photoc – fotolia.com;
**Stand:** Oktober 2012

# **Viele Herausforderungen:** Eine Antwort

Weltweit haben sich die Informations- und Netzwerktechnologien rasant weiterentwickelt und damit sowohl die Verhaltensweisen als auch die Arbeits- und Geschäftsprozesse der Menschen maßgeblich verändert. Viele Arbeitsschritte sind durch die digitalen Medien schneller und kostengünstiger geworden. Das Internet ist heute praktisch unverzichtbar.

Den unbestrittenen Vorteilen der Internetnutzung stehen aber auch Risiken gegenüber. Die Anzahl der Straftaten im Bereich Cybercrime steigen seit Jahren weltweit rasant an, wobei immer mehr Wirtschafts- und Lebensbereiche davon betroffen sind. Da im „world wide web" nationale Grenzen keinerlei Rolle spielen, kann sich auch Österreich dieser Entwicklung nicht entziehen.

Die Bekämpfung dieses neuen Kriminalitätsfeldes bedarf daher auch neuer Strategien. Denn mit den bisherigen Ermittlungs- und Beweissicherungsmethoden wird zukünftig keine ausreichende Bekämpfung dieser steigenden Kriminalitätsform mehr möglich sein.

Aus diesen Gründen war es notwendig entsprechende Strategien zu erstellen, um diesen Entwicklungen entgegen zu wirken. International wurden deshalb bei Interpol, Europol sowie auf nationaler Ebene, wie zum Beispiel Deutschland und Frankreich, moderne Zentralstellen, so genannte Kompetenzzentren eingerichtet, um eine koordinierte und effektivere Bekämpfung von Cybercrime zu ermöglichen.



In Österreich wurde das Bundeskriminalamt (.BK) mit der Erstellung einer umfassenden Gesamtstrategie zur Bekämpfung von Cybercrime in Österreich betraut.
Eine Cyber-Sicherheitsstrategie kann nur dann erfolgreich sein, wenn alle betroffenen Akteure gemeinsam ihre jeweilige Aufgabe wahrnehmen. Die Cyber-Strategie des Innenministeriums ist daher so aufgebaut, dass zukünftig in der gesamten Polizeistruktur die Bekämpfung der Internetkriminalität einen Schwerpunkt einnimmt. Ziel ist es, den Herausforderungen im Bereich Cybercrime mit einer effizienten Struktur, adäquatem Know-How der Mitarbeiterinnen und Mitarbeiter sowie modernster technischer Ausstattung, aber auch durch mögliche Kooperationsformen mit relevanten externen, nationalen und internationalen Akteuren, entsprechend zu begegnen. Zentraler Bestandteil dieser Gesamtstrategie ist die Errichtung eines modernen und vernetzten Cybercrime-Competence-Center, kurz „$C^4$" genannt, im Bundeskriminalamt.

Mag.ª Johanna Mikl-Leitner
Bundesministerin für Inneres

General Franz Lang
Direktor des Bundeskriminalamts

# **Der Inhalt:** Das Verzeichnis

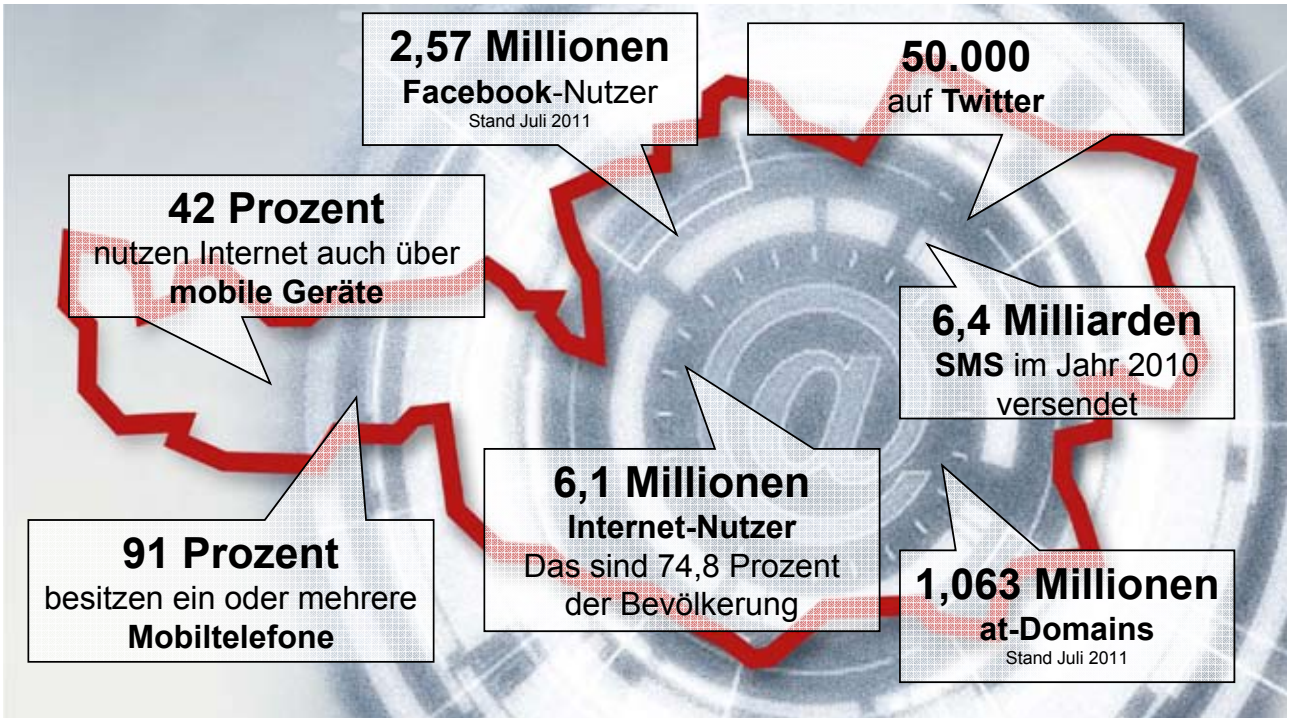
# **Die digitale Welt:** Neue Informationstechnologien verändern unser Leben

In den letzten zehn Jahren hat das Internet weltweit eine starke Verbreitung erlangt. Laut „Internet World Stats" gab es im Jahr 2000 bereits weltweit mehr als 361 Millionen Internetzugänge, bis zum Jahr 2011 ist diese Zahl auf über zwei Milliarden angestiegen.

Auch in den österreichischen Haushalten hat der Einsatz von Informations- und Kommunikationstechnologie (IKT) in den letzten Jahren stark zugenommen. Beispielsweise waren im Jahr 2011 bereits 75 Prozent der Haushalte mit einem Internetzugang versorgt.

Für die heimische Wirtschaft ist das Internet zu einem wichtigen Marktplatz geworden. Immer mehr Unternehmen setzen mit einer eigenen Website auf eine verstärkte Vernetzung und auf Internetpräsenz. 2011 verfügten rund 98 Prozent der Unternehmen über einen Internetzugang.

Social Media Plattformen wie Facebook und Twitter haben durch die rasant ansteigenden Nutzerzahlen eine große Bedeutung im Leben vieler Menschen erlangt. Facebook, als bekannteste Social Media Plattform, erreichte in Österreich bis Ende 2011 rund 2,6 Millionen registrierte Userinnen und User.




Eine repräsentative Studie über die Onlinenutzung durch Kinder und Jugendliche (Forschungsverbund EU Kids Online, Jänner 2011) zeigt den enormen Stellenwert des Internets bei dieser Zielgruppe: 98 Prozent der neun- bis 16-jährigen Kinder in Österreich nutzen das Internet zuhause, 48 Prozent im eigenen Kinderzimmer. 53 Prozent der Befragten nutzen das Internet via Mobiltelefone oder Smartphones, 62 Prozent haben ein eigenes Profil innerhalb eines sozialen Netzwerks im Internet.

Aber nicht nur das Internet, sondern auch die rasche Entwicklung neuer Technologien, wie zum Beispiel Mobiltelefone, verändern unsere Verhaltensmuster und Kommunikationsformen. Bereits 2009 waren 91 Prozent der österreichischen Haushalte zumindest im Besitz eines Mobiltelefons. Der Anteil an Smartphones in Österreich ist dabei bis zum Jahr 2011 auf rund 21 Prozent angestiegen. Nicht zuletzt, weil immer mehr Kriminelle die Möglichkeiten dieser multifunktionalen Geräte zu schätzen wissen, erlangen mobile Geräte aber auch in der polizeilichen Arbeit immer mehr an Bedeutung.

# **Cyberkriminalität in Österreich:** Auch die Verbrecher gehen mit der Zeit


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.

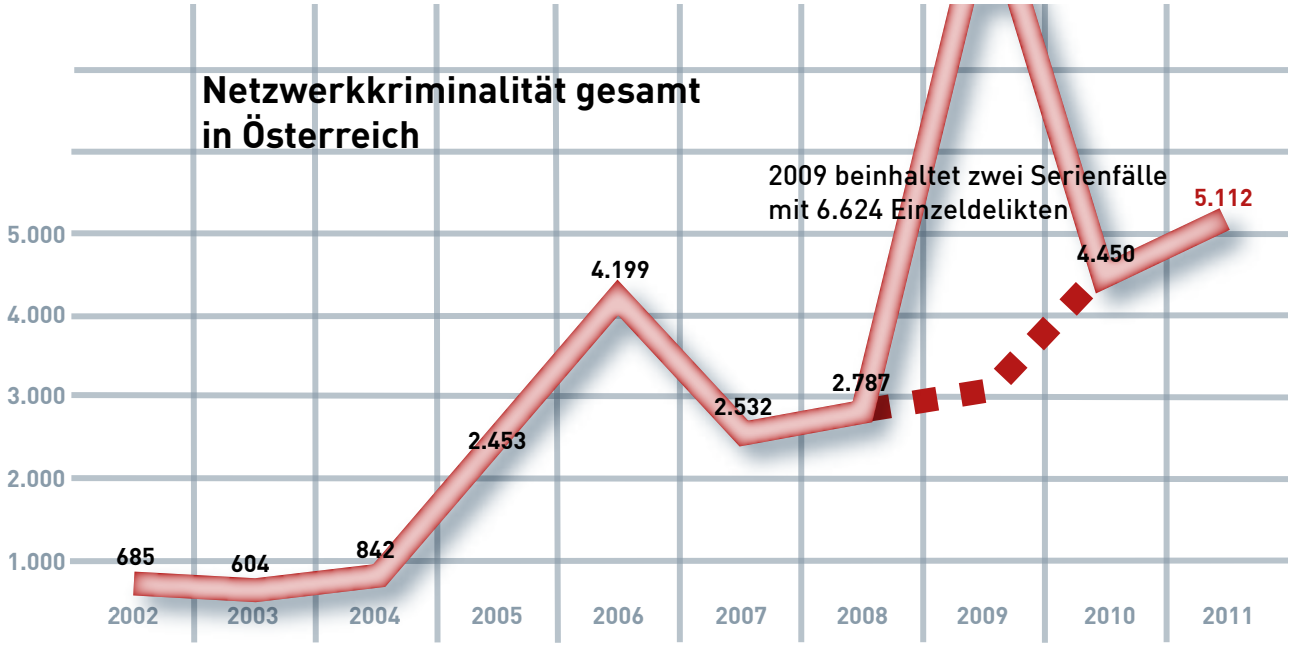


Für Kriminelle wird das Internet immer attraktiver, ständig entstehen neue Deliktsformen und kriminelle Bedrohungen im Netz. So erlangte 2011 der Begriff des „Hacktivismus" durch Datenlecks sowie Angriffe auf renommierte Unternehmen und Institutionen Einzug in den Sprachgebrauch. Cyberkriminelle haben auch den Bereich der mobilen Endgeräte für sich entdeckt und weiten ihre Attacken auf diese aus. Mittlerweile ist der Internetbetrug im Bereich der organisierten Kriminalität lukrativer als andere riskantere Formen der Kriminalität. Die Motive für viele Cyberdelikte sind neben finanziellen Interessen nach wie vor Langeweile und Geltungsdrang sowie vermehrt auch das Erregen medialer Aufmerksamkeit.

## **Zahlen und Fakten:** sprechen eine deutliche Sprache

Das Internet ist ein ideales Werkzeug für Kriminelle. Mit wenig Aufwand erreichen die Täter mit einem Mausklick potentielle Opfer auf der ganzen Welt. Das wahre Ausmaß des Schadens, der durch Cyber-Kriminelle verursacht wird, lässt sich deshalb nur schwer erfassen. Europol schätzt ihn jährlich auf 750 Milliarden Euro weltweit. Nach wie vor muss aber von einer sehr hohen Dunkelziffer ausgegangen werden. 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.

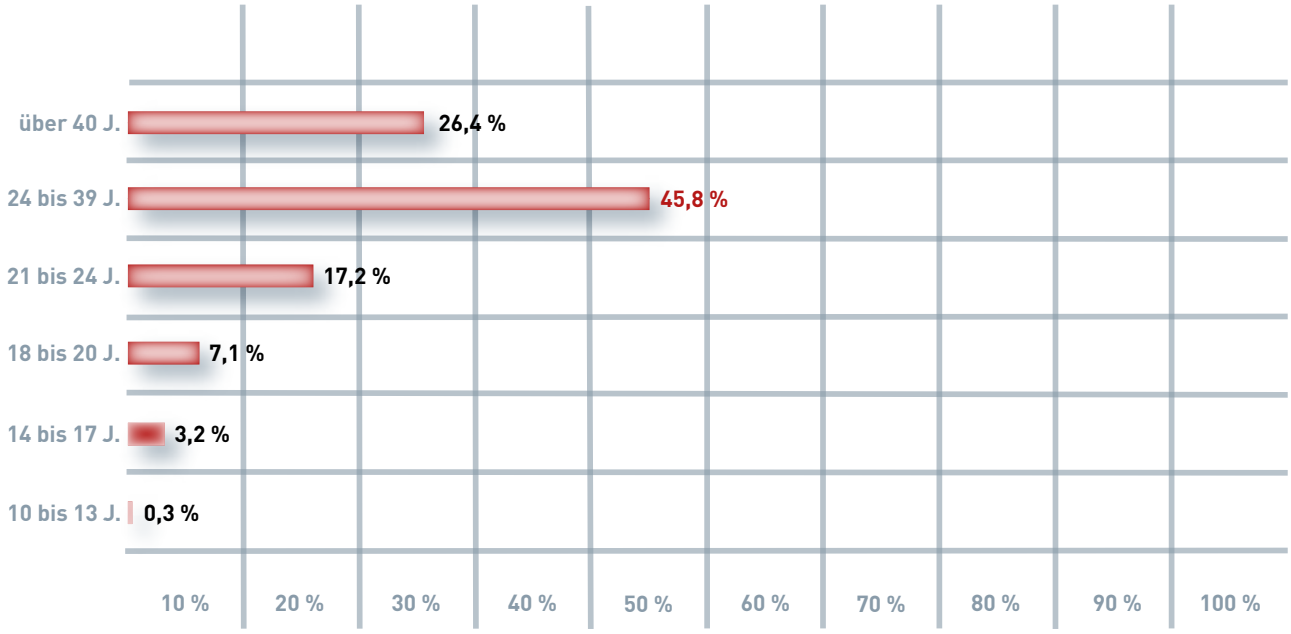
Trotz dieser Umstände war, wie bereits in der Vergangenheit, auch im Jahr 2011 ein weiterer Anstieg der Kriminalität im Netz statistisch feststellbar.



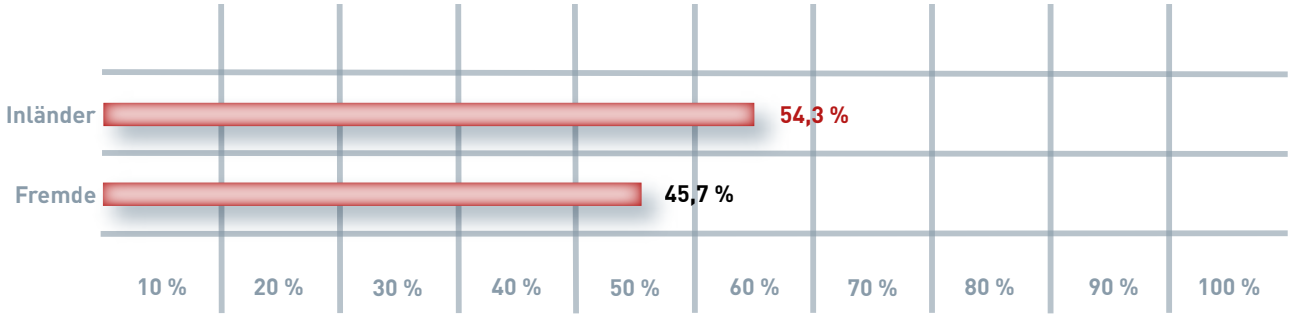



Die Aufklärungsquote lag 2011 durchschnittlich bei 43,7 Prozent, was einem Rückgang von rund fünf Prozent gegenüber 2010 bedeutet. Dies ist einerseits auf die Professionalisierung der Tätergruppierungen, die kriminell organisiert und international vernetzt sind, und andererseits auf die schwierige und langwierige Ermittlungsarbeit bei Cybercrime-Delikten zurückzuführen.

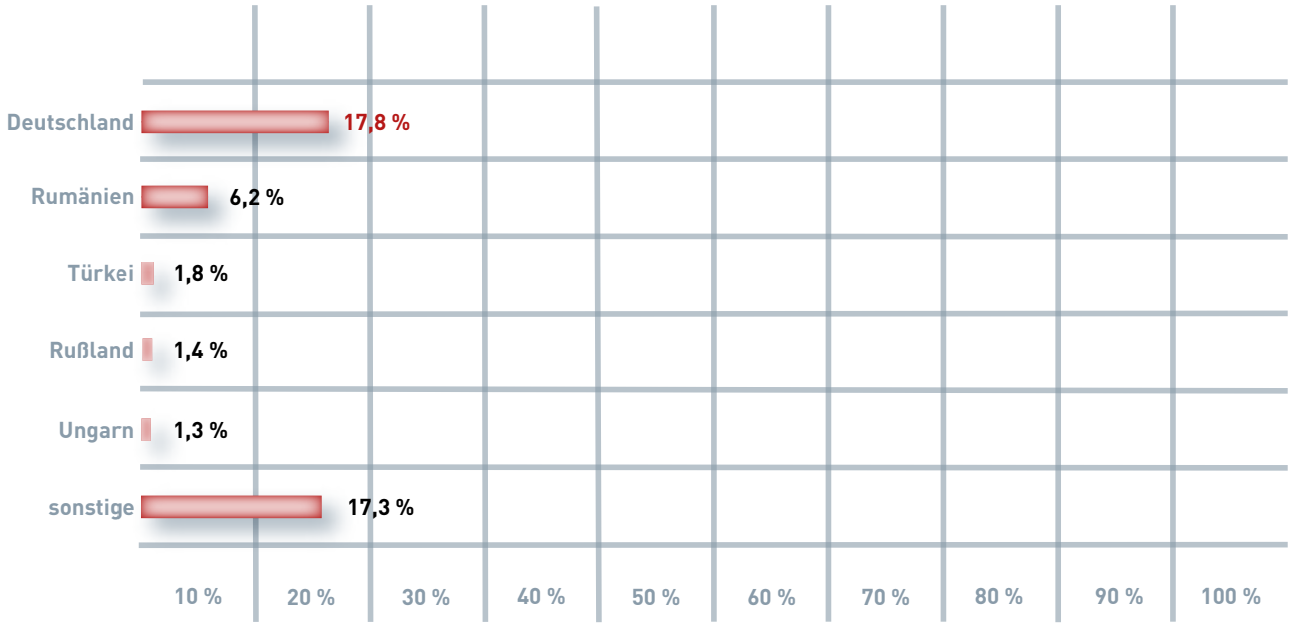
Bei den Tatverdächtigen ist, mit rund 46 Prozent, die stärkste Gruppe die der 25- bis 40-Jährigen, gefolgt von den unter 25-Jährigen mit rund 28 Prozent und den über 40-Jährigen mit rund 26 Prozent.



Von den ermittelten Tätern stammen mit rund 54 Prozent mehr als die Hälfte aus dem Inland.



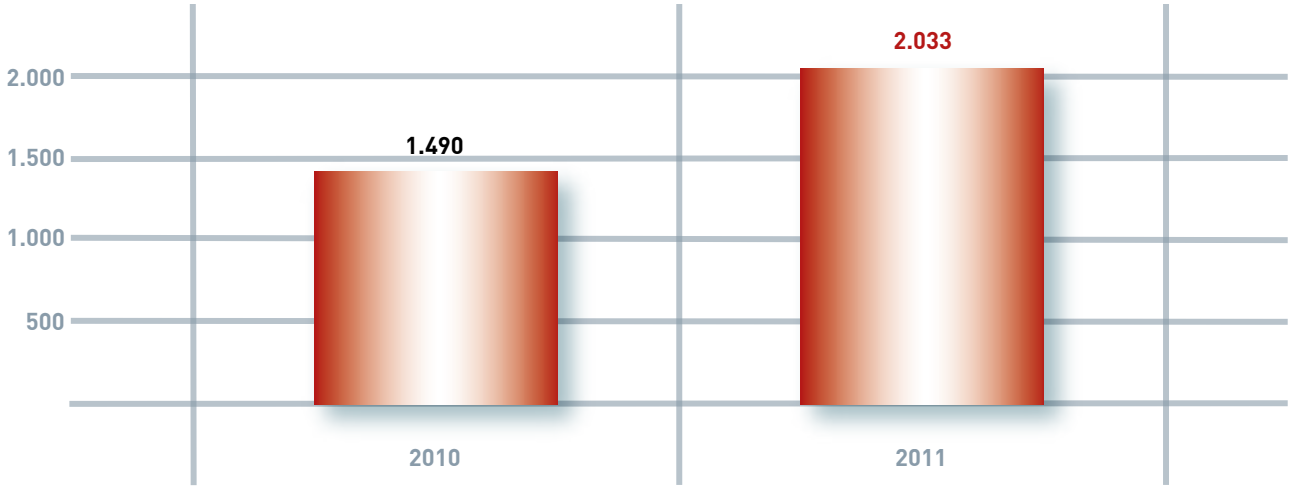

Der Anteil an Nicht-Österreicherinnen und Nicht-Österreichern beträgt rund 46 Prozent, wobei Deutschland mit rund 18 Prozent und Rumänien mit rund sechs Prozent den größten Anteil stellen. Hier wirkt sich die räumliche und sprachliche Nähe zu Deutschland, vor allem bei den Betrugsfällen im Internet, aus. Ansonsten ist schwerpunktmäßig eine Verteilung der Täter im osteuropäischen Raum zu erkennen.



# **Die Tricks der Computerkriminellen:** Motive Geld und Aufmerksamkeit

## 1. Betrugsdelikte

Ein Großteil der Straftaten im Internet entfällt auf Betrugsdelikte. Das Internet bietet für die Täter den Vorteil der Anonymität, der größeren Reichweite und der Sorglosigkeit der Bevölkerung im Umgang mit persönlichen Daten. Vielfach sitzen die Täter im Ausland bzw. verschleiern ihre digitale Spur, wodurch eine Verfolgung für die Strafverfolgungsbehörden erschwert wird. Gerade im Bereich des Internetbetrugs kam es im Jahr 2011 zu einem starken Anstieg im Vergleich zum Vorjahr: der Betrug durch Missbrauch des Internets stieg von 2010 auf 2011 um rund 36 Prozent auf insgesamt 2.033 Anzeigen.






Wie gehen die Täter vor? Beim Internetbetrug wird das Internet zur Kontaktherstellung mit potenziellen Opfern benutzt. Dabei werden beispielsweise nicht existente Waren, vor allem Kraftfahrzeuge, Elektroartikel oder Kommunikationsgeräte angeboten. Das Ziel der Täter ist die Erwirkung einer Vorauszahlung von den Opfern. Dabei gibt es die verschiedensten Erscheinungsformen, darunter:

### Bestellbetrügereien

Wie gehen die Täter vor? Hierbei werden Waren mit dem Vorsatz bestellt, diese nicht zu bezahlen. Vielfach werden falsche Namen angegeben bzw. die versandten Pakete mit einer falschen Unterschrift angenommen. Da der Name des Betrügers falsch ist und dieser auch nicht unter der angegebenen Adresse wohnt, kann die Forderung zumeist nicht eingetrieben werden.

### „Lovescam“ oder „Datingscam“

Wie gehen die Täter vor? Dabei versuchen zumeist ausländische Betrügerinnen und Betrüger durch das Vortäuschen einer fiktiven Liebesgeschichte vom Opfer Geld zu erhalten. Die Täter nehmen unter anderem über Singlebörsen Kontakt mit den Opfern auf und spielen diesen vor, sie hätten sich verliebt, wobei sie nach einiger Zeit unter einem Vorwand um Geld bitten. So bitten sie beispielsweise um Geld für die Reise zu einem gemeinsamen Treffen, für Heilungskosten der Betrügerin oder des Betrügers oder auch eines nahen Angehörigen oder für andere Ausgaben, um den Kontakt aufrechterhalten zu können.

### Finanzagenten oder „Money Mules“

Wie gehen die Täter vor? Eine Finanzagentin oder ein Finanzagent stellt ihr oder sein Konto zur Verfügung, auf welchem Gelder empfangen und weitertransferiert werden, die aus kriminellen Machenschaften stammen. Oftmals werden diese über Nebenjobangebote (beispielsweise mit dem

Betreff „Arbeit für dich“) angeworben. Dabei werden dem Finanzagenten 20 Prozent des auf sein Konto transferierten Betrages als Gewinn versprochen. Die überwiesenen Gelder stammen dabei zumeist von Personen, die selbst Opfer krimineller, zumeist betrügerischer Handlungen wurden. Die Finanzagentin oder der Finanzagent dient lediglich dazu, die Spur des Geldes zu verschleiern und die illegal erlangten Gelder möglichst schnell und über möglichst viele Stationen ins Ausland zu transferieren. Derartige Angebote klingen meist sehr verlockend, man kann sich dabei jedoch der Mittäterschaft zur Geldwäscherei oder des Betrugs strafbar machen.

### Gewinnversprechen

Wie gehen die Täter vor? Mittels E-Mail, aber auch postalisch, werden Gewinnverständigungen versandt, wobei jedoch vor Inanspruchnahme des angeblichen Gewinns die Überweisung eines Geldbetrags, der für die Freigabe des Gewinns sowie für diverse Zahlungen erforderlich ist, verlangt wird.  Generell gilt, wer an einer Lotterie nicht teilgenommen hat, kann üblicherweise auch nicht gewinnen. Dennoch fallen immer wieder Menschen auf vermeintliche Gewinnverständigungen herein.

### Fake-Webshops

Wie gehen die Täter vor? Ein Täter oder eine Tätergruppe eröffnet gefakte, also vorgetäuschte Webshops und bietet Waren jeglicher Art zum Kauf an. Die Käufer bezahlen die Kaufsumme, die nicht-existenten Waren werden jedoch nie geliefert. Von den Tätern werden Serverstandorte in Ländern gewählt, die behördliche Ermittlungen erheblich erschweren, größtenteils sogar unmöglich machen. Gleichzeit werden Techniken genutzt, um die Herkunft und Identität zu verschleiern, bereitgestellt durch sogenannte Bulletproof – Provider, das sind Anbieter, die ihre Kunden mit einem Server-Standort versorgen, der sicher vor Zugriffen internationaler Ermittlerinnen und Ermittler ist. Die Shops existieren nur wenige Wochen, danach verschwinden sie wieder.



## Polizei-Erfolg:
## Haupttäter in Österreich festgenommen

2011 konnte, nach eineinhalbjährigen Ermittlungen in einer gemeinsamen Aktion mit dem Bundeskriminalamt Wiesbaden und dem Bayerischen Landeskriminalamt eine Tätergruppe ausgeforscht werden, die rund 800 gefälschte Webshops betrieben und mehrere tausend Opfer geschädigte hatte. Ein Haupttäter dieser Gruppe war Österreicher und konnte in seiner Wohnung in Niederösterreich festgenommen werden. Der angerichtete Schaden wird mit einem zweistelligen Millionenbetrag beziffert.

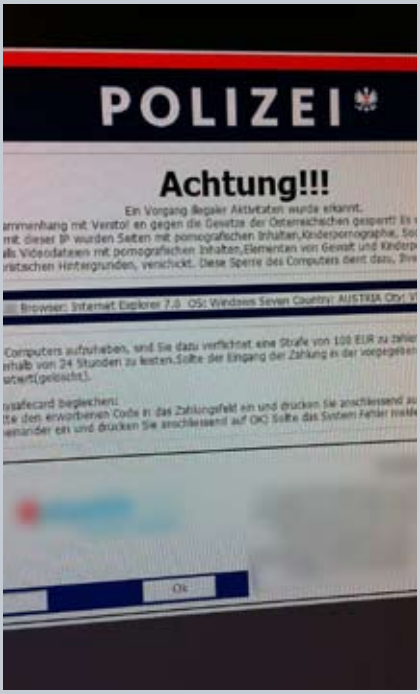
## 2. Viren, Würmer, Spyware, Trojaner-Programme

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 „Polizei-Virus“:** Ein europaweites Phänomen

**Das Bundeskriminalamt ermittelt aktuell gegen eine Tätergruppe, die mit der Verbreitung von sogenannter „Ransomware“ im Internet aktiv ist. Dabei wird Schadsoftware verschickt, die Computersysteme sperrt und die Userinnen und User auffordert, für die Freigabe des Personal Computers (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.

## 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 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 in ihren Arbeitsgruppen mit der Bekämpfung dieses Phänomens befasst.



## 4. Phishing

Beim 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.

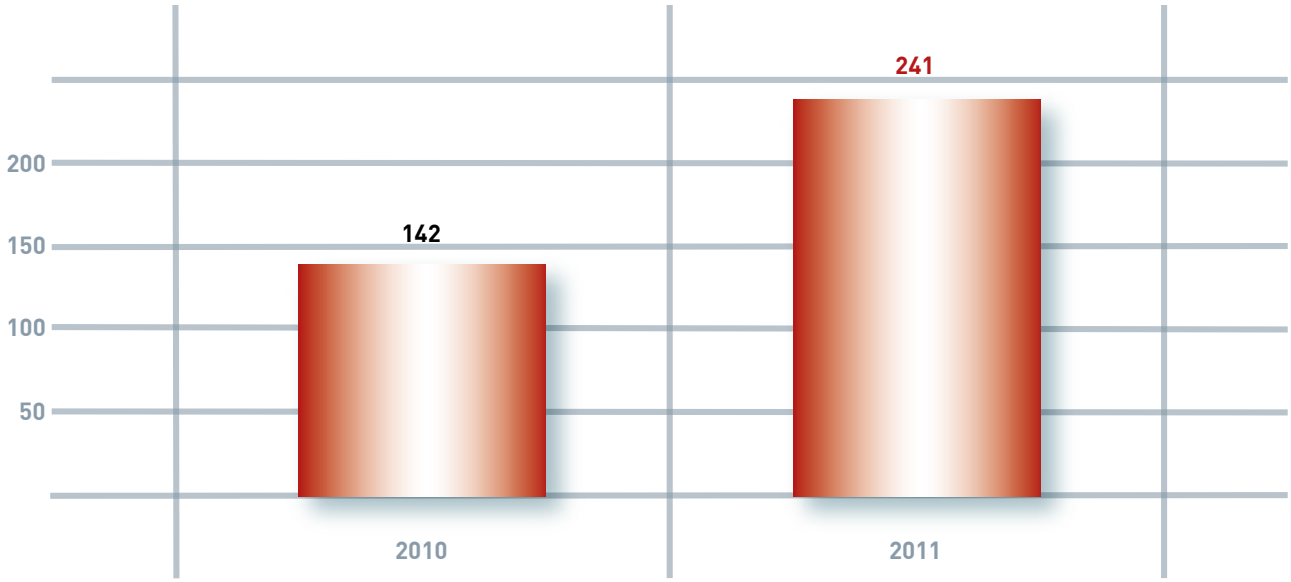

Das Phänomen des Phishings beschäftigt die österreichische Exekutive bereits seit Ende

2005. Ab Mitte des Jahres 2007 war in Österreich – entgegen den internationalen Trends – ein starker Rückgang von Phishingfällen feststellbar. Seit kurzem wird aber wieder ein Ansteigen der Anzeigen registriert, was vor allem auf neue Varianten von Trojaner-Programmen, die nunmehr auch in Österreich aktiv sind, zurückzuführen ist.

Die angezeigten Fälle von Phishing stiegen innerhalb eines Jahres um 167 Prozent auf 184 Anzeigen an.

## 5. Hacking

Unter Hacking versteht man die Schaffung eines unberechtigten Zugangs zu Computersystemen unter Umgehung der Sicherheitssysteme. Ziel der Hacker ist die Überwindung der Sicherheitsmechanismen um Schwachstellen aufzudecken oder für ihre Zweke auszunützen. Als Motiv geben die Täter einerseits kriminelle Motive wie Betrugsabsicht oder andererseits Langeweile, Geltungsdrang oder Nachahmung an. Von 2009 auf 2011 haben sich Anzeigen im Bereich des Hackings mit 241 Fällen mehr als verachtfacht. Ursächlich für diesen Anstieg dürften eine verbesserte „Anzeigemoral" in der Bevölkerung sowie die Zunahme von Hackingfällen in sozialen Netzwerken sein.






### 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. wurden vor allem durch Malware, Hacker und Personen aus dem Lebensumfeld angegriffen. Ungeeignete Passwörter, zu viel Vertrauen, 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

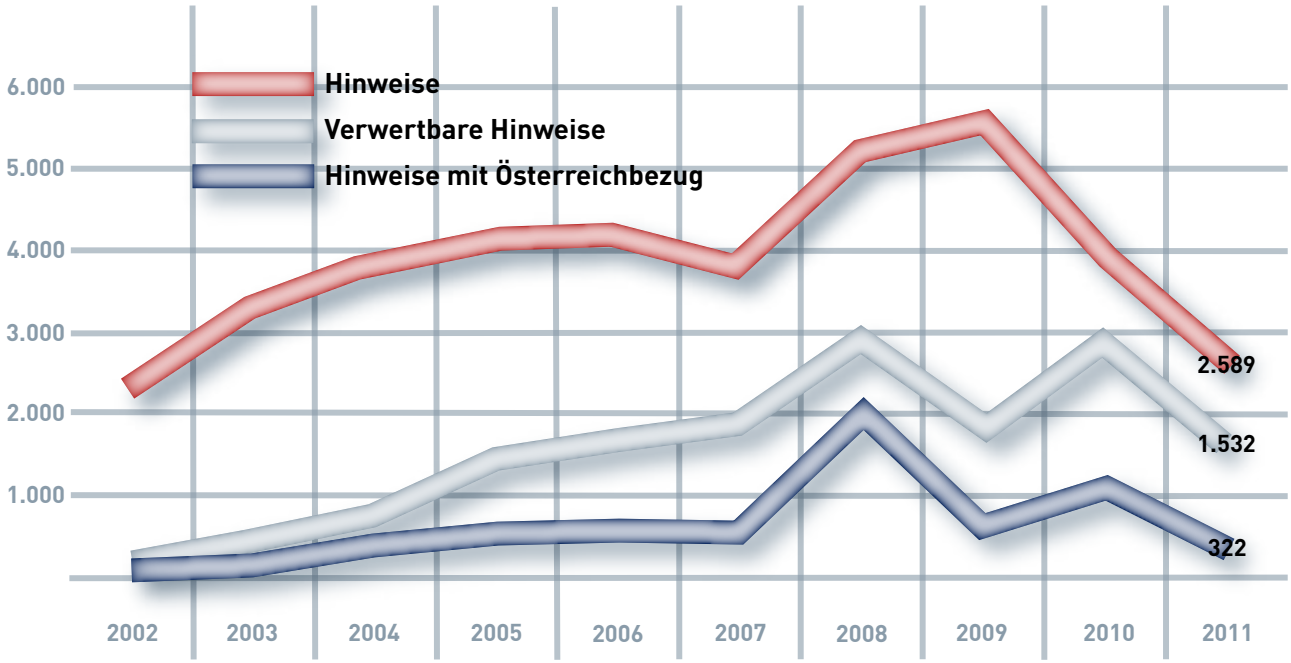
Login-Informationen wird in vielen Fällen die Identität missbraucht, um befreundeten und bekannten Personen beispielsweise eine Notlage vorzutäuschen und somit Geldüberweisungen zu veranlassen. Die Täter löschen nach dem E-Mailversand alle Kontakte und vergeben ein neues Passwort, damit der eigentliche 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 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 (Pornografische Darstellung Minderjähriger) ist in § 207a Strafgesetzbuch (StGB) unter Strafe gestellt und umfasst die Herstellung, Verbreitung, das Verschaffen, den Besitz und den Zugriff. Laut der Kriminalstatistik Österreich ist die Zahl der Anzeigen von 315 im Jahr 2010 auf 502 Anzeigen im Jahr 2011 angestiegen. Mit 1. Jänner 2012 wurde der neue § 208a Strafgesetzbuch „Anbahnung von Sexualkontakten zu Unmündigen“ als neuer Straftatbestand für Cybergrooming im österreichsichen Strafrecht eingeführt.

In der im Bundeskriminalamt eingerichteten Meldestelle für Kinderpornografie und Kindersextourismus (interpol@meldestelle.at) sind im Jahr 2011 insgesamt 2.589 Hinweise bearbeitet worden, wovon 322 Hinweise Österreichbezug aufwiesen.






Durch die steigende Anzahl von Web2.0-Anwendungen steht Internetusern 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, stattdessen aber das kinderpornografische Material verstärkt auf geschlossenen Foren und Chats unter anderem in sozialen Netzwerken ausgetauscht wird. Diese Tatsache bewirkte auch einen Rückgang privater Hinweise an die Meldestelle.

Diesem massiv anwachsenden Ausweichtrend der Szene auf so genannte „Filesharingprogramme“ sowie „File hosting services“ und „Bulletin Boards“ begegnet die Kriminalpolizei und erhöht in diesem Bereich ihren Verfolgungsdruck.

Weiters ist eine starke Verlagerung auf „peer-to-peer-Dienste“, wie etwa „eDonkey“ feststellbar. Diese Dienste beruhen auf dem Prinzip des direkten Kontaktes, sodass die Identität der User nicht über einen zentralen Anbieter, sondern nur durch aktives Tauschen von illegalem Material und Erfassung der Netzwerkverbindung festgestellt werden kann.

Die Beobachtung der Opfer ergab im Jahr 2011 – wie auch in den Vorjahren – einen anhaltenden Trend zu Opfern aus dem ehemaligen Ostblock. Vielfach konnte auch eine verstärkte Tendenz zu immer jüngeren Opfern und brutaleren Missbrauchsszenen festgestellt werden.

## **Operation GHOSTRIDER:** Erfolgreicher internationaler Schlag gegen Kinderpornografie im Netz

**Nach Ausforschung und Festnahme eines österreichischen pädokriminellen Täters konnten auf Grund seiner Chatkontakte im Internet, Hinweise auf insgesamt weitere 197 Täter festgestellt werden.**

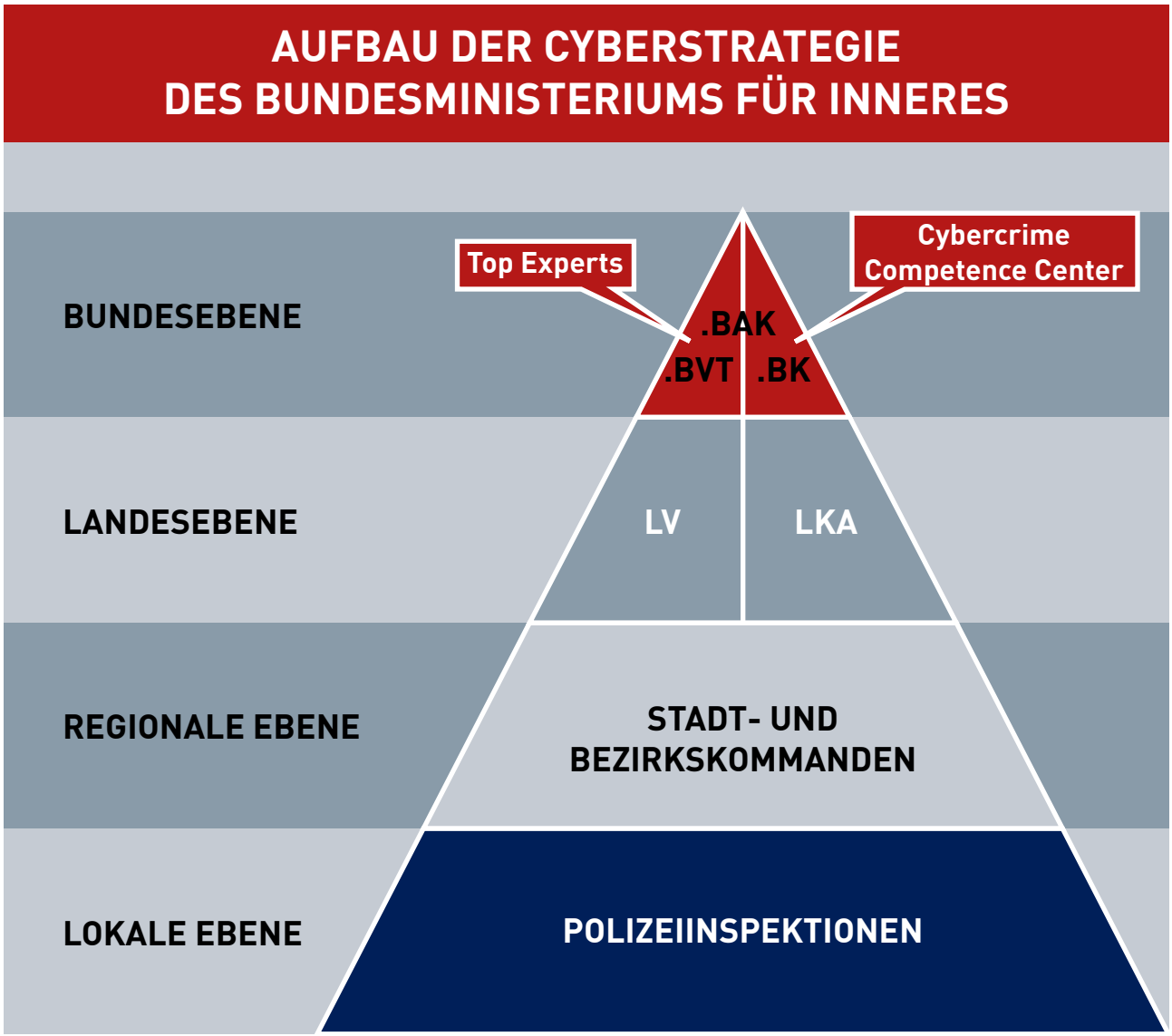
In enger Zusammenarbeit mit dem Landeskriminalamt Wien und der Staatsanwaltschaft Wien konnten darunter 25 Österreicher im Alter von 19 bis 75 Jahren ausgeforscht und an die Justiz übergeben werden. Die Täter versuchten in diversen Chats und sozialen Netzwerken Kontakt zu Kindern zu erlangen. Sie erschlichen sich ihr Vertrauen und forderten sie anschließend auf, sich vor der Webcam nackt auszuziehen bzw. selbst Nacktbilder anzufertigen und an die Täter zu übermitteln. Die Polizei konnte zwei Tätern nicht nur die Verbreitung kinderpornografischen Materials, sondern auch die Vergewaltigung von Kindern

nachgeweisen. Ein 55-jähriger Niederösterreicher wurde wegen Vergewaltigung und Kindesmissbrauch an einem 13-jährigen Buben zu vier Jahren Haft verurteilt. Ein 47-jähriger Niederösterreicher wurde wegen Vergewaltigung an zwei minderjährigen Buben und Widerstand gegen die Staatsgewalt zu fünf Jahren Haft verurteilt. Weiters konnte im Zuge der neunmonatigen Operation eine Gruppe von insgesamt weiteren 74 Tatverdächtigen ermittelt und die Namen an die zuständigen deutschen Behörden ausgehändigt werden. Eine weitere Gruppe bestehend aus 98 tatverdächtigen Personen wurde an die amerikanischen Ermittlungsbehörden weitergeleitet.

# **Die Cybercops:** Im Team gegen die IT-Kriminellen

Eine Cyber-Sicherheitsstrategie kann nur dann erfolgreich sein, wenn sie umfassend gestaltet ist und alle betroffenen Akteure gemeinsam ihre jeweilige Aufgabe wahrnehmen. Für den Bereich Cybercrime wurden daher folgende Ziele definiert:

- Drohende Gefahren in Bezug auf Cybercrime müssen frühzeitig erkannt werden, um so
- rasche Maßnahmen zur Gefahrenabwehr treffen und
- Gefahrenquellen und Verursacher ausforschen zu können.
- Die Erkenntnisse aus den kriminellen Aktivitäten fließen umgehend in die präventiven Maßnahmen ein.




Die Bekämpfung von Cybercrime wird seitens der Exekutive auf allen Ebenen verstärkt: auf lokaler Ebene in den rund 900 Polizeiinspektionen und in den 111 Bezirks- und Stadtpolizeikommanden, wobei hier der Fokus im Präventionsbereich sowie der Verbesserung von Ausbildungsmaßnahmen liegt. Auf Ebene der Bezirke und der Landeskriminalämter erfolgen weitere Spezialisierungen und eine Bündelung des Know-hows. Mit der Einführung sogenannter Bezirks-IT-Ermittler wird 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.

# Aus- und Weiterbildung: Kompetente Ansprechpartner

Die Aus- und Weiterbildung der Internetpolizistinnen und –polizisten nimmt einen hohen Stellenwert in der gesamten Sicherheitsstrategie ein und erfolgt daher auf allen Ebenen:

- Die Polizistinnen und Polizisten auf der Ebene der Polizeiinspektionen, der Stadtpolizeikommanden und der Bezirkspolizeikommanden erhalten im Rahmen ihrer Grundausbildung, bei der Ausbildung zur dienstführenden Beamtin oder zum dienstführenden Beamten sowie im Rahmen von Fortbildungsmaßnahmen IT-Basisschulungen. Sie sind die ersten Ansprechpartner für die Bevölkerung und fordern – sofern notwendig – die Expertinnen und Experten der Landeskriminalämter beziehungsweise des Bundeskriminalamts zur Unterstützung an. In einigen Bundesländern wird bereits das so genannte Modell der Bezirksdatensicherer umgesetzt. Dabei handelt es sich um Polizeibeamtinnen und -beamte, die durch das jeweilige Landeskriminalamt eine Zusatzausbildung und eine Praxisschulung erhalten haben. Sie unterstützen das jeweilige Landeskriminalamt bei der Datensicherung auf lokaler Ebene und sind erste Ansprechstelle für die Polizeiinspektionen. Dieses Modell hat sich bewährt und soll daher im Rahmen der Cybercrime-Strategie flächendeckend in Österreich umgesetzt werden.

- Auf lokaler und regionaler Ebene sind geschulte Präventionsbeamtinnen und –beamte verfügbar. Im Jahr 2011 wurden diese in Kooperation mit der Wirtschaftskammer geschult, um insbesondere für Klein- und Mittelbetriebe kompetente Ansprechpartner zu sein. Außerdem wird das Thema Cybercrime im Rahmen der Kriminaldienstfortbildungsrichtlinie (KDFR) behandelt. Vortragende sind sowohl interne Experten des Bundeskriminalamts als auch externe Spezialistinnen und Spezialisten.



- Auf Länderebene sind in den Landeskriminalämtern speziell ausgebildete Exekutivbeamtinnen und -beamte, so genannte IT-Forensiker, tätig. Diese verfügen über eine polizeiliche Ausbildung und werden zusätzlich im IT-Bereich geschult und fortgebildet. Die Schulungen werden unter anderem auch in Kooperation mit der Wirtschaft abgehalten, um auch hier „up to date“ zu sein. Über die Basisausbildung hinaus finden Fortbildungsschulungen in Form von Workshops statt.

- Die Ausbildung der Beamtinnen und Beamten auf Bundesebene (Bundeskriminalamt und Bundesamt für Verfassungsschutz und Terrorismusbekämpfung) erfolgt im Rahmen nationaler und internationaler Schulungen. So ist das Bundeskriminalamt an mehreren internationalen Schulungsprojekten beteiligt. Internationale Organisationen, wie zum Beispiel die „International Association for Computer Information Systems“ (IACIS), ein Zusammenschluss von polizeilichen Forensikexpertinnen und –experten, führen Grundausbildungen und Spezialmodule im Rahmen europäischer Projekte durch. Weiters ist das Bundeskriminalamt am europäischen Schulungsprogramm „European Cybercrime Training and Education Group“ (ECTEG) im Bereich Hightech-Crime beteiligt. Im Rahmen einer zweijährigen akademischen Ausbildung am University College Dublin wird der Abschluss als Master of Science in Computer Forensic and Internet Investigation angeboten. Im Jahr 2011 hat ein Beamter des Bundeskriminalamts diese Ausbildung mit dem Masters Degree abgeschlossen und steht nunmehr national als Trainer zur Verfügung. Zusätzlich finden externe, nationale Schulungen zur laufenden Fortbildung im Bereich Betriebssysteme, Auswertungssoftware und Server und Netzwerke statt. Außerdem erfolgen anlassbezogene Schulungen und Workshops unter anderem mit Microsoft oder dem Computer Emergency Response Team (CERT).

- Das Bundeskriminalamt kooperiert weiters mit nationalen Hochschulen: so besteht im Rahmen des KIRAS-Programms - ein österreichisches Förderprogramm für die Sicherheitsforschung - eine Kooperation mit der Fachhochschule St. Pölten (Projekt „Steg-IT“). Gemeinsam mit der Donau-Universität Krems und der Universität Wien wurde das Projekt „Cyber Stalking“ bereits erfolgreich abgeschlossen.

# Cybercrime-Competence-Center "C⁴": Das Headquarter


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. Dort werden Expertinnen und Experten unter Verwendung moderner Technologien und innovativer Arbeitsmethoden an der Bekämpfung von Cybercrime arbeiten. „Technologiemonitoring" ermöglicht es auf neue Entwicklungen und damit einhergehende Gefahren frühzeitig reagieren zu können. Im „C⁴" soll auch ein technischer Support für die nachgeordneten Dienststellen sichergestellt werden. Überdies können die Prozesse bei der Cybercrime-Bekämpfung durch die Nutzung von Synergieeffekten beschleunigt werden. Das Cybercrime-Competence-Center 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. Eine Besonderheit des Cybercrime-Competence-Centers ist die Einbindung zweier weiterer Organisationseinheiten des Bundesministerium für Inneres (BM.I), dem Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) und dem Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung (BAK) sowie die Implementierung einer Schnittstelle in den Bereich Cyber-Security, wodurch ein rascher Informationstransfer zwischen diesen einzelnen Bereichen gewährleistet wird.

Das Cybercrime-Competence-Center wird in erster Linie die Funktion einer zentralen Schnitt- und Meldestelle sowohl innerhalb der polizeilichen Organisation als auch für Bürgerinnen und Bürger übernehmen und versteht sich als die internationale Ansprechstelle im Zusammenhang mit Cybercrime.



Derzeit befindet sich das „C⁴" in der Phase der Umsetzung. Im Endausbau wird es folgende Organisationsstruktur aufweisen:

## 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<br>Ausbildung<br>Analyse und Schnittstelle zu Wirtschaft und Forschung Technik | IT-Forensik<br>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. Im Laufe des Jahres 2011 sind rund 1.300 Meldungen zu Vorfällen im Internet in der Meldestelle eingegangen, wobei diese vor allem folgende Sachverhalte betreffen:

- Internetbetrugsfälle mit eher geringen Schadenssummen (zum Beispiel nicht gelieferte aber bezahlte Bestellungen auf diversen Plattformen wie Ebay, Willhaben etc.)
- Betrügerische „Lockangebote“ zum Beispiel auf Willhaben oder Ebay
- Bloße Hinweise auf Internetseiten, die dem Absender verdächtig erscheinen
- Massenmails, die an Postfächer Privater gesendet werden (419er-Briefe, Lotteriegewinne, etc.)

### 2. Erfassung, Analyse und Auswertung digitaler Spuren

Die Spezialistinnen und Spezialisten in den Landeskriminalämtern und des „C$^4$“, die so genannten IT-Forensikexpertinnen und -experten, werden immer dann aktiv, wenn besondere Fälle von Computerkriminalität aufzuklären sind oder zur Unterstützung, wenn polizeiliche Ermittlungen, technische Erhebungen erforderlich machen 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 es jetzt weiter zu intensivieren und auszubauen gilt. 2011 wurden folgende Initiativen erfolgreich gestartet bzw. umgesetzt:

- **Projekt „IT-Sicherheit“:** Rascher Informationsausaustausch zwischen dem Bundesministerium für Inneres und der Wirtschaftskammer Österreich (WKO)

Wirksame Maßnahmen zur IT- und Datensicherheit für heimische Unternehmen werden immer wichtiger, da das Gefahrenpotential von Cyberattacken ständig zunimmt. Mit dem gemeinsamen Projekt „IT-Sicherheit“ des Bundesministeriums für Inneres und der Wirtschaftkammer Österreich soll im Bereich „IT-Sicherheit“ zur Bewusstseinsbildung, durch das Aufzeigen von Bedrohungsszenarien, beigetragen und Hilfe bei der Entwicklung von Sicherheits- und Servicepaketen in Kombination mit Schulungsmaßnahmen, geleistet werden. Dazu wurde ein Informationsfolder erstellt und eine Internetplattform sowie IT-Sicherheitshandbücher von der Wirtschaftskammer Österreich zur Verfügung gestellt. Weiters werden von der Wirtschaftskammer Österreich Warnmeldungen des Bundeskriminalamts auf der Internetplattform „IT-Safe“ 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


- **Gemeinsame Aus- und Weiterbildung:** Schulungen von Präventionsbeamtinnen und –beamten in Kooperation mit der Wirtschatskammer Österreich

2011 schulte das Bundeskriminalamt gemeinsam mit der Wirtschaftskammer Österreich insgesamt 300 Präventionsbeamtinnen und -beamte aus ganz Österreich (100 Beamtinnen und Beamte aus Wien, 42 aus Niederösterreich, 16 aus dem Burgenland, 20 aus Kärnten, 30 aus der Steiermark, 35 aus Oberösterreich, 25 aus Salzburg und je 16 aus Tirol und Vorarlberg) über die gesetzlichen Rahmenbedingungen, Datenschutz, IT-spezifische Themen mit praktischen Beispielen als auch über Gefahren, die aktuelle Bedrohungslage und Lösungsansätze im Bereich der IT-Kriminalität. Die Präventionsbeamtinnen –und beamten arbeiten auf lokaler und regionaler Ebene in den Polizeiinspektionen und sind im Bereich der Eigentumskriminalität insbesondere auch für Klein- und Mittelbetriebe erste Ansprechpartner.

**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“. 2011 fand diese Veranstaltung in Wiesbaden statt. Ziel dieser international anerkannten Expertenkonferenz ist es, innovative Projekte und Technologien mit polizeilicher Relevanz (Schwerpunt IT und Internet) vorzustellen und eine Brücke zwischen Wissenschaft und Forschung sowie den polizeilichen Praktikern zu schlagen. Renommierte Organisationen und Forschungsinstitute haben hier bereits innovative Projekte und Forschungsergebnisse vorstellen können 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 User und die polizeiliche Arbeit geprüft und beurteilt werden.

**Kooperation mit Hochschulen und universitären Einrichtungen:** Neues Know-how

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-Forensiker des Bundeskriminalamts auch zu internationalen Schulungsaktivitäten wie zum Beispiel der „European Cybercrime 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. Hervor zu heben ist der Abschluss eines Mitarbeiters des Bundeskriminalamts mit einem Master of Sience am University College in Dublin in dem Themengebiet „Computer Forensics and Cybercrime Investigations“ im Herbst 2011 sowie die Teilnahme von zwei IT-Forensikern an der International-Summerschool am University College in Dublin. Darüber hinaus wird derzeit gemeinsam mit der Fachhochschule St. Pölten und weiteren Projektpartnern am KIRAS-Projekt „StegIT“ über steganografische Verfahren in Kommunikationsvorgängen gearbeitet.



## 4. International verbündet

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 Europäische Union (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 entschieden, ein Europäisches Zentrum zur Bekämpfung von Cyberkriminalität bei Europol einzurichten. Zudem werden in vielen Staaten, wie zum

Beispiel in Deutschland, Frankreich und Belgien eigene Cybercrime-Zentren aufgebaut um die gegenseitige Vernetzung zu verbessern. In Österreich übernimmt diese Rolle das Cybercrime-Competence-Center im Bundeskriminalamt. Nur durch eine enge Vernetzung von spezialisierten Zentralstellen kann eine qualifizierte und schnelle Reaktion auf Vorfälle im Bereich Cybercrime und Cybersecurity erreicht werden.

**Europol**

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**

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 Cybercrime 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.



# **Service:** So hilft die Polizei

Nur keine Scheu: 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

**Die Kriminalpolizei dokumentiert alle tatrelevanten Daten anhand der vorgelegten Unterlagen – so etwa die Absenderangaben in der Kopfzeile von E-Mails oder Computerprotokolle.**

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.

## Vorsorgen ist besser als heilen

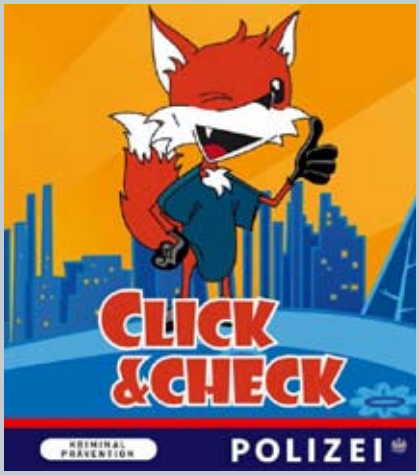
Für die Polizei hat beim Thema „IT-Sicherheit“ die Prävention einen hohen Stellenwert. Durch verstärkte, kompetente und rasche Präventionsarbeit kann viel zur Sicherheit jedes einzelnen im Internet beigetragen werden. Denn viele Betrugshandlungen und Angriffe auf IT-Systeme könnten bei entsprechender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

In vielen Veröffentlichungen und Veranstaltungen liefert die Prävention 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 Internet und der sozialen Medien verbunden sind, zu verbessern. Ein Schwerpunkt der polizeilichen Vorsorgeaktivitäten ist die Information über technische Schutzmaßnahmen. Solche Systemsicherungen sollen einem Angreifer das Eindringen in die Informationstechnologie so schwermachen, dass der von ihm zu betreibende Aufwand größer ist als der zu erwartende Nutzen.

## „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 wollen ihre Identität ausbilden. 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.




**Happy slapping**

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 2011 wurden österreichweit über 13.200 Jugendliche von 749 Präventionsbeamtinnen und –beamten darüber informiert. Dieses erfolgreiche Projekt wird im Jahr 2012 weiter ausgebaut werden.

### Beratung im Internet

Auf der Webseite und auf den Facebook-Seiten des .BK 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.

## Kriminalprävention in den Landeskriminalämtern

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

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



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

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

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

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

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

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

**Landeskriminalamt Wien**
Kriminalprävention
Wasagasse 22
1090 Wien
Tel.: 01/31310/37250
E-Mail: LPK-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: LPK-W-LKA-AB-Kriminalpraevention@polizei.gv.at

# **Ausblick:** Neue Chancen, neue Risiken, neue Herausforderungen

Seit Jahren sind die Strafverfolgungsbehörden bei der Bekämpfung von Cybercrime mit einer zunehmenden Professionalisierung und Kommerzialisierung seitens der Täter konfrontiert. Die rasanten technologischen Entwicklungen sowie die Verbreitung der sozialen Netzwerke durch das Web2.0 führten zu einer Präsenz des Internets in unserem Alltag, die vor wenigen Jahren noch nicht vorstellbar war. Diese Omnipräsenz des Internets spiegelt sich auch in der steigenden Anzahl der Anzeigen als auch in den Protestaktivitäten der „Hacktivisten" wider.

Mit dem Missbrauch von IT-Systemen lässt sich sehr viel Geld verdienen. Mittäter für kriminelle Aktivitäten suchen und finden sich dabei in einschlägigen Internetforen. Persönliche Kontakte gibt es kaum. Dazu kommt der zunehmende Einsatz technischer Hard- und Software wie etwa Verschlüsselungssoftware und Anonymisierungsdienste für kriminelle Zwecke. Aufgrund der Internationalität dieser Kriminalitätsform und dem völligen Fehlen nationaler Grenzen kann sich kaum ein Land der IT-Kriminalität entziehen, so auch nicht Österreich. Es ist daher für die kriminalpolizeilichen Ermittlungen und die Erkenntnisgewinnung von größter Bedeutung die Kontakte zu ausländischen Dienststellen, insbesondere auch außerhalb Europas, weiter auszubauen.

Bei Ermittlungen im Zusammenhang mit Wirtschaftskriminalität oder Kinderpornografie sind für die Auswertungen der sichergestellten Datenmengen moderne Netzwerke, leistungsfähige Rechner und eine aktuelle Software von größter Bedeutung. Nur so lässt sich der Zuwachs der ständig steigenden Datenmengen einigermaßen kompensieren.

Die Polizeibehörden weltweit haben die Erfordernisse nach einer schnelleren Reaktion auf Cyberattacken und besserem Know-how bei der Verfolgung erkannt und errichten Zentralstellen zur Bündelung der Kompetenzen. Auf internationaler und europäischer Ebene manifestiert sich diese Entwicklung in der Errichtung des Europäischen Cybercrime Centre EC3 bei Europol und des Digital Crime Center IDCC bei Interpol.

Parallel zu diesen Entwicklungen wurde im Jahr 2011 die Errichtung des österreichischen Cybercrime-Competence Centers, kurz „$C^4$" im Bundeskriminalamt beschlossen. Seine volle Wirkung kann das „$C^4$" allerdings nur dann entfalten, wenn es Teil eines bundesweiten, ganzheitlichen Lösungsansatzes ist, weshalb ihre Einrichtung in eine, alle Ermittlungsebenen umfassende, Gesamtstrategie eingebettet ist.

In einigen Ländern wurden für die Verfolgung von Cybercrime-Delikten spezialisierte Staatsanwaltschaften eingerichtet. Die damit erzielten Erfolge lassen dieses Beispiel für Österreich nachahmenswert erscheinen.

# **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

42 Prozent der Österreicherinnen und Österreich haben im vergangenen Jahr Waren und Dienstleistungen über das Internet bestellt. 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.

## Sicher auf Facebook, SchülerVZ & Co.

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: Erläuterungen

**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.

**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 dabei entweder physikalisch oder – heute meist – logisch zwischen den beiden Kommunikationspartnern und hat dabei mit seinem System komplette Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern 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.

**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.

**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

# Notizen: Anmerkungen

# Notizen: Anmerkungen

BUNDESKRIMINALAMT