Humanitas Helvetica e.V.
Newsletter

Kinder und Jugendliche als Opfer und Täter von Cyberkriminalität

Richard Benda, Präsident Vereinigung Kriminaldienst Österreich VKÖ

Erfreulicherweise geht die Kriminalität in ihrer Gesamtheit überall in Europa zurück. Eine Art der Kriminalität - die Cyberkriminalität - folgt nicht diesem Trend, im Gegenteil, sie vermehrt sich fast explosionsartig. Erhebt sich zwangsläufig die Frage, wie weit sind Kinder und Jugendliche gefährdet und wie oft treten sie als Täter in Erscheinung?

Laut Schweizer Kriminalstatistik für 2016 stagniert die Zahl der Verurteilten bei knapp unter 110‘000. Auch die Zahl der verurteilten Jugendlichen bleibt stabil bei einer Höhe von 12‘090 Verurteilungen. Die Jugendkriminalität hat somit einen Anteil von nicht ganz 11 %. Der Anteil von jugendlichen Straftätern ist anscheinend auch in anderen Ländern ähnlich.

4‘841 Kinder unter 14 Jahren und 23‘499 Jugendliche zwischen 14 und 17 Jahren wurden in Österreich 2016 als Täter ausgeforscht - Tendenz steigend. Von der Gesamtsumme aller strafrechtlichen Delikte (270‘160), hat damit die Jugendkriminalität einen Anteil von nicht ganz 10%. Die Frage ob der Anteil jugendlicher Täter bei Cyberdelikten ähnlich ist, ist noch nicht geklärt. Anzunehmen ist, dass auch hier die Tendenz steigend ist, denn Konflikte unter Jugendlichen verlagern sich von der direkten, persönlichen Konfrontation via Facebook und Snapchat auf das Internet. Ca. 20% der Kinder haben bereits vor Schulbeginn Zugang zum Internet. Die Zahl erhöht sich bei 14jährigen auf 80%. Kinder und Jugendliche als Täter und Opfer bei Cyberkriminalität sind daher wahrscheinlich.

Bei Cyberkriminalität, also bei Delikten die ausschliesslich über Internet und Online begangen werden können, denken die meisten Menschen an so genannte High-Tech-Kriminalität. Hacker mit universitärer Ausbildung, hochbegabt und motiviert greifen Netzwerke von Behörden und Firmen an. Diese Art wird auch als Cyberkriminalität im engeren Sinn bezeichnet.

Kinder und Jugendliche wird man bei diese Art der Kriminalität natürlich nicht finden, diese Altersgruppe bewegt sich im so genannten Low-Tech-Bereich. Diesem Bereich wird auch die Mehrheit der Fälle von Cyberkriminalität zugerechnet. Klassisches Beispiel ist hier z. B. der Diebstahl einer Bank- oder Kreditkarte. Erst mit deren Verwendung wird aus einem einfachen Diebstahl ein Cyberdelikt. Häufiger sind aber Kinder und Jugendliche Opfer und auch Täter bei Delikten, die sowohl in herkömmlicher Art, als auch mit Hilfe von Computer, Internet und Online begangen werden können. Typisch dafür sind Mobbing, Stalking und Sexting, auf die noch eingegangen wird.

Die Täter

Die Feststellung wie weit Kinder, also Personen unter 14 Jahren, im Bereich Cyberkriminalität Täter sind, ist nicht festzustellen. Kinder sind nicht strafbar, es gibt also keine Verurteilungen und auch sonst liegen über Kinder keine empirischen Daten vor. Anders sieht es bei Jugendlichen aus, sie findet man bereits in der Kriminalstatistik und sie scheinen auch schon bei wissenschaftlichen Untersuchungen als

Das häufigste Delikt im Computerbereich ist Mobbing. (Bild © Fotolia; #35068545; Gina Sanders)

4‘841 Kinder unter 14 Jahren und 23‘499 Jugendliche zwischen 14 und 17 Jahren wurden in Österreich 2016 als Täter ausgeforscht - Tendenz steigend. (Bild © Fotolia; #187064702; triocean)

Täter auf (Studie der Donau-Universität Krems, Cyberkriminelle in Wien - 2006-2016). Bei jugendlichen Tätern muss man unterschiedliche Vorgangsweisen und Motivationen unterscheiden. Da wären die „Jung-Hacker“, die auch als Skriptkiddies bezeichnet werden. Es sind Jugendliche, meist im Alter von 14-16 Jahren, die mit wenig Wissen über die Materie dennoch grossen Schaden anrichten können. Sie versuchen in jugendlichem Forscherdrang in Datensysteme einzudringen und verursachen dort eher aus Unwissenheit als mit Vorsatz Schäden. Begangen werden mit dieser Tathandlung die Delikte des „Widerrechtlichen Zugriffes auf fremde Computersysteme“, „Löschen von Daten“, „Störung der Funktionsfähigkeit eines Computersystems“ oder „Verletzung des Telekommunikationsgeheimnisses“ vor allem aber „Datenbeschädigung“. Skriptkiddies sind aber eher in der Minderheit unter den jugendlichen Cyberkriminellen.

Die Mehrheit sind Jugendliche die aus Rache, Eifersucht oder Schadenfreude gezielte Angriffe gegen Gleichalterige starten. Zu unterscheiden sind zwei Arten: Eine Gruppe verwendet soziale Netzwerke um ihr Opfer zu mobben, die andere verschafft sich Zugang zu Passwörtern oder Geräten und manipuliert Smartphone oder Computer.

Ein nicht zu unterschätzender Faktor jugendlicher Cyberkriminalität wird durch die Tathandlung der Verletzung des Urheberrechtes begangen. Logos, Bilder oder Musik werden kopiert, wobei die Jugendlichen sich meist nicht bewusst sind, dass sie damit das Delikt der Urheberrechtsverletzung begehen.

Während die Täter bei der Computerkriminalität ohne Altersunterscheidung Männer weit überwiegen (in Österreich 83,2%), ist dies in der Altersklasse unter 18 Jahren nicht so offensichtlich. Da es hier kaum statistisches Material gibt sind nur Schätzungen möglich. Nach Angaben von Ermittlern in diesem Bereich ist der Anteil von weiblichen Tätern jäh nach Delikt sehr unterschiedlich. Bei gewissen Delikten wie Mobbing könnten sogar Mädchen überwiegen. Das Cybermobbing, das ausschliesslich über soziale Medien betrieben wird, kein Spass ist, zeigen Fälle bei denen Opfer in den Selbstmord getrieben wurden.

Beachtenswert ist, dass Cyberkriminelle ihre Delikte fast immer mit einer falschen Onlineidentität ausführen.

Die Opfer

Die Motivation des Täters ist die wichtigste Frage bei der Opferwerdung. Im Bereich der Cyberkriminalität liegt unangefochten die Geldgier und Gewinnstreben an erster Stelle. Bei jugendlichen Tätern scheint diese Motivation dagegen eher selten. Im Fokus stehen nicht finanzielle, sondern persönliche Motive. Firmen, Behörden oder Personen öffentlichen Interesses findet man als Opfer bei Jugendlichen eher nicht. Der Angriff richtet sich immer gegen Privatpersonen, meist im ähnlichen Alter und ist deshalb immer persönlich und skalpellartig. Als Opfer werden aber auch nicht selten Lehrer, Erzieher oder Trainer auserkoren, auf jeden Fall Personen zu denen ein persönliches Verhältnis besteht. Häufig wird ihnen sexuell abartiges Verhalten vorgeworfen.

Die Delikte

In vielen Fällen ist Naivität und der leichtsinnige Umgang mit Daten ein offenes Einfallstor für **Identitätsdiebstahl**. Unter Jugendlichen werden häufig digitale Passwörter ausgetauscht, was in der Folge dazu führen kann, dass der eigene Account ausspioniert wird. Es wird auch häufig vergessen, dass alles was in das Netz eingespeichert wird, gegen die Person selbst verwendet werden kann. Die Täter von Identitätsdiebstahl können zahlenmässig nicht eruiert werden, weil sie sich in der Regel hinter Delikten wie Diebstahl, Betrug etc. verbergen.

Ein Jugendtrend, das **Sexting** (Weitergabe von Nacktfotos oder Fotos mit erotischem Inhalt), hat schon häufig zu

Cyberattacken geführt. Nacktfotos die bei intakter Verbindung vielleicht anregend wirken, werden nicht selten bei Beendigung der Beziehung in das Netz gestellt und führen dann zu entsprechender Häme in sozialen Netzwerken. Sexting wird nur in den wenigsten Fällen angezeigt und wenn verbirgt es sich in Delikten wie Nötigung oder Erpressung. Eine Ausfilterung bei diesen Delikten nach Motiv erfolgt in keiner Statistik. Man kann aber einen Teil beim § 207a Strafgesetzbuch (Kinderpornografie) vorfinden. Erstaunlich, dass man bei dem Delikt **Kinderpornografie** auch jugendliche Täter findet. In Österreich wurden 2016 648 Fälle angezeigt. Als Tatverdächtige konnten immerhin 56 Kinder und 45 Jugendliche ausgeforscht werden. Vermutlich liegen bei diesen Tätern keine pädophile Neigung oder finanzielle Interessen vor, sondern jugendlicher Leichtsinn. Trotzdem Pornofilm bleibt Pornofilm.

Jedenfalls stellen bei den 4‘537 begangenen Delikten gegen die sexuelle Integrität die Jugendlichen einen Anteil von 553 Tatverdächtigen, also einen Anteil von 12%. Ein Teil davon wird durch Tathandlungen im Cyberraum ausgeführt.

Das wohl häufigste Delikt im Computerbereich ist **Mobbing**. Start ist meist eine falsche Anschuldigung oder eine Verleumdung, die sich zu Psychoterror entwickelt. Wiederholt und regelmässig werden falsche Tatsachenmitteilungen gepostet. Die Anschuldigungen im Netz werden meist direkt in der Schule oder am Arbeitsplatz wiederholt und enden oft in direkten körperlichen Angriffen. Befragungen von Schülern ergaben, dass ca. 20% der Schüler Cybermobbing ausgeliefert sind. Laut Kriminalstatistik 2016 wurden in Österreich aber lediglich 12 Kinder und 47 Jugendliche Opfer von Mobbing. Bemerkt werden muss, dass aber viele Delikte dieser Art nicht angezeigt werden und wohl eher beim Psychologen oder Psychiater enden. Wenn man die geringe Zahl von jugendlichen Mobbingtätern jenen der Gesamtzahl von 271 gegenüberstellt, ergibt sich doch ein Prozentsatz von ca. 21%.

Die kriminellere Form von Mobbing sind **Verhetzung und Verleumdung** über digitale Medien. In diesen Fällen wird meist nicht eine Person, sondern eine Gruppe, eine Rasse, eine Religion der öffentlichen Kritik durch Falschmeldungen ausgesetzt. Natürlich können diese Delikte auch auf andere Weise gesetzt werden, doch durch die rasante Vervielfältigung ist das Internet das beste Medium für diese Delikte. Ziel ist es durch gezielte falsche Informationen Shitstorms auszulösen und die Gruppe damit öffentlicher Häme auszusetzen.

Phising und Pharming sind eine Betrugsmethode die von Kriminellen gerne angewendet werden und denen Jugendliche in ihrer Naivität nur allzu leicht zum Opfer fallen. Die Opfer werden bei Besuch von kriminellen Websites aufgefordert persönliche Daten und Passwörter anzugeben. Kein seriöser Anbieter verlangt das. Ob dadurch Identitätsdiebstahl vorgenommen wird oder der Computer Teil eines Booth-Netzes wird, hängt dann von Kriminellen ab. ●

Ein typischer Fall

Der männliche Teil eines jugendlichen Liebespaares ist eifersüchtig und versucht seine Freundin zu überwachen. Wie ginge es besser, als sich Zugang zu ihrem Computer zu verschaffen. Nach mehrmaligem Drängen ist das Mädchen so leichtsinnig und gibt ihm das Passwort für ihr Mobiltelefon. Mit dem Wissen, dass die meisten Menschen ein Passwort für alle digitalen Möglichkeiten verwenden, loggt er sich im Namen des Mädchens in einen Chatroom ein. Unter einem anderen Pseudonym legt er ein eigenes Profil in dem Chatroom, der ausschliesslich für Mädchen sein sollte, an. Er nimmt unter dem Pseudonym Kontakt mit seiner Freundin auf und bringt sie dazu ihm laszive Fotos zu schicken. Sie glaubte ja, dass sie diese einem gleichaltrigen Mädchen senden würde. Als nach einiger Zeit die Verbindung in Brüche geht, veröffentlicht der Ex-Freund die Fotos in einem Chatroom ihrer Schule. Der Blossstellung folgt noch Mobbing durch Schulkameraden.

In vielen Fällen ist Naivität und der leichtsinnige Umgang mit Daten ein offenes Einfallstor für Identitätsdiebstahl. (Bild © Fotolia; #62903211; Wordley Calvo Stock)

Impressum

Humanitas Helvetica e.V. - Newsletter

Herausgeberin
Humanitas Helvetica e.V.
Mimosenstrasse 5, 8057 Zürich
http://www.humanitas-helvetica.ch

Verantwortlicher Redaktor
Hans-Ulrich Helfer
helfer@humanitas-helvetica.ch

Layout, Website
Swisswebmaster GmbH
info@swisswebmaster.ch

Erscheinungsweise
Regelmässig als Print- oder Online-Ausgabe.

Bezug, Unterstützung
Website: www.humanitas-helvetica.ch
Unkosten- und Unterstützungsbeiträge bitte auf Postcheckkonto: 85-587554-5:
IBANCH50 0900 0000 8558 7554 5
Vermerk: „Spende“

Druck
Eigendruck

Copyright
Alle Rechte vorbehalten.

Kindesmissbrauch

Schweigen oder Anzeigen?

Humanitas Helvetica e.V.

www.humanitas-helvetica.ch

Bild: © Fotolia; #75040420; Gina Sanders