3 - 2 - 1: meins! 1 - 2 - 3: Betrügerei!

Internetkriminalität

Von Jörg-Michael Klös, Kriminaldirektor, Berlin

Jörg-Michael Klös
Kriminaldirektor, Berlin

Überall in der Stadt sieht man sie. An Plakatwänden auf den Bahnhöfen, als Annoncen in den Zeitungen oder Zeitschriften, auch in Gestalt von Großpostern an den Litfaßsäulen. Geradezu euphorisch blicken sie drein, die Frauen und Männer, eher den jüngeren Jahrgängen zuzurechnen, denen die Anspannung ob der gecounteten Sekunden drei zwei eins noch im Gesicht geschrieben steht. Der Höhepunkt der Dramaturgie erreichte bei Zero fast schon eine schicksalhafte Dimension. Mein oder dein, alles oder nichts, Sekt oder Selters! Schließlich die Auf- und Erlösung: meins! Na toll, denkt der Betrachter, hat ja dann wohl geklappt, das mit dem Schnäppchen. Sollte ich auch mal probieren...

Bei mir weckt dieses Plakat allerdings regelmäßig andere Impulse. Zugegeben, ich bin seit über 30 Jahren Polizeibeamter und somit „jobgeschädigt“. Da muss man sich wohl nicht wirklich schämen, wenn die Gedankengänge selten dem zu folgen bereit sind, was fremdbestimmt vordergründig assoziiert werden soll.
Im Laufe des Berufslebens hat unsereins eben über Empirie, auch Trial and Error, gelernt, dass das Gute dem Menschen keinesfalls wesensimmanent ist,
im Gegenteil. Die Dinge hinterdenken, skeptisch sein, Verdacht schöpfen – das ist somit selbstverständlicher, fast schon automatischer Bestandteil der eigenen Lebensphilosophie und -strategie geworden, nicht nur im Beruf. Das kann warnen und schützen, durchaus aber auch lähmen und mitunter belasten. Risikominimierend ist es allemal, spontanitätshemmend aber ebenfalls. Der Hang dazu, den (vermeintlich) sicheren Weg gehen zu wollen, überwiegt.
Irgendwie haftet einem dadurch das Label des „Langweilers“ an. Damit kann man leben. Richtig, der Prototyp eines ebay-Kunden bin ich nicht. Schade eigentlich – manchmal. Andererseits laufe ich so nicht Gefahr, disponiertes oder gar prädisponiertes Opfer der Internetkriminalität zu werden. Auch damit kann ich leben und zwar gut. Denn: Wer garantiert mir, dass sich auf den beschriebenen Plakaten tatsächlich die glücklichen Ersteigerer einer begehrten Sache mit pekuniärem oder ideellem Wert präsentieren? Vielleicht sind da ja die abgebildet, und verbreiten ihr strahlendes Siegerlächeln, die die Offerte gemacht hatten. Und zwar ein Angebot, das in Wirklichkeit keines war, zumindest kein ehrliches. Ein Scheingeschäft eben oder ein Geschäft, das nur im Sinne des Verkäufers diesen Namen verdient. Minderwertige Ware, funktionsuntüchtige bzw. beschädigte Gegenstände, Falsifikate, gestohlene oder unterschlagene Sachen. Denn auch der Betrüger hat als ebay-Kunde nachvollziehbar Grund zur Freude, geht es ihm doch ausschließlich um das Geld der Auktionäre. Genau das bekommt er nach dem Countdown mit Geschick und Glück. Drei – zwei – eins: meins!

Sicherlich ist es weder sachgerecht noch fair, das Internet pauschal oder die Domäne ebay speziell zu kriminalisieren und zu diskreditieren. Gleichwohl liefert das Internet erhebliche Räume und Nischen für ein ganzes Sammelsurium
unterschiedlichster Kriminalitätsfelder. Und das in einer Dimension, die aufhorchen lässt.
Die Dunkelfeldschätzung der Fachleute liegt bei einer Größenordnung von 1 -
2 % inkriminierter Seiten des Internetangebotes. Was auf den ersten Blick nicht signifikant aussieht, erweist sich bei näherer Betrachtung gegenteilig. Etwa 100.000 Newsgroups und aktuell deutlich mehr als eine Milliarde (!) Webseiten im Cyberspace lassen die 1 – 2 % in einem anderen Licht erscheinen.

Hinzu kommt, dass das Internet schon seit Jahren und weiterhin ungebrochen expandiert. Je mehr Webnutzer sich in das Netz begeben desto mehr Täter, aber auch Opfer, wird es hervorbringen. Die Tatgelegenheiten steigern sich schier ins Grenzenlose, gleich dem Charakter des Internet als universelles Kommunikations- und Interaktionssystem selbst. Zweifellos sind da die staatlichen Organe gefordert, wenn sich ins Unkontrollierbare abgleitende und sich jeder Schranke oder Sozialregelung entziehende Entwicklungen abzeichnen. Das gilt für die Legislative, Judikative und Exekutive gleichermaßen. Bei dem rasanten Tempo der Fortschritte auf dem Gebiet der Technik, der enormen innovativen Kreativität auch der leider nicht nur seriösen Internetnutzer, den erheblichen Differenzen bei der Rechtslage in den Ländern, die ja problemorientiert weltweit zu betrachten wäre, und der zunehmend festzustellenden Bereitschaft einer Vielzahl von geradezu hasardierenden, mit einer Art Goldgräbermentalität operierenden Glücksritter, die vor lauter €-

und $ - Zeichen in den Augen kaum noch den 19“-Monitor visuell fixieren können, sind den staatlichen Einflussmöglichkeiten und Regulierungsoptionen Grenzen gesetzt. Das bezieht sich auf personelle wie auf ausstattungsbezogene Ressourcen. Hinzu kommt das Thema Zeitmanagement. Selbst bei einer möglicher-weise zu erreichenden weitgehenden Harmonisierung der Rechtslage: Wer will und kann denn die Inhalte der Internetseiten bzw. deren Angebote auch nur annähernd umfassend und gegenwartsbezogen prüfen? Welche Polizei oder sonstige Institution soll das leisten?

Bei einem erheblichen Teil der Internetkriminalität handelt es sich um so genannte Kontrolldelikte, da existiert weder ein Anzeigender noch Geschädigter. Ob Staatsschutzdelikte, Rauschgiftkriminalität, Produktfälschung oder Vertrieb/Besitz von Kinderpornografie, um nur einige Beispiele zu nennen, immer ist und bleibt die Polizei auf sich gestellt.
Die zweite Seite der Medaille – gemeint sind die Delikte, die sehr wohl Primäropfer hervorbringen und somit Strafanzeigen, die die Polizei gemäß dem Legalitätsprinzip per se zu verfolgen hat – stellt die Ermittlungsbehörde gleichermaßen vor Kapazitäts-, mitunter aber auch vor Akzeptanzprobleme. Nicht selten entsteht der Eindruck, dass die Bereitschaft der Inkaufnahme eines erhöhten und zumeist unverhältnismäßigen Sicherheitsrisikos von Seiten der Beteiligten proportional zu der erwarteten/erhofften Gewinnmaximierung steigt. Da werden auch Gelder an völlig unbekannte Geschäftspartner transferiert, ohne dass erforderlichenfalls auch nur der Hauch einer Chance zur Identifizierung real wäre. Geht’s gut – prima! Geht’s schief, ruft man nach der Polizei.

Aber auch ganze Industrie- und Vertriebsunternehmen gehen zunehmend dazu über, in punkto Sicherheit stringent nach dem Kosten-Nutzen-Prinzip zu verfahren. Weniger Betriebskosten rechtfertigen allemal Abstriche am Kontrollsystem. Entsprechende Einbußen werden kalkuliert und sind im Preisgefüge berücksichtigt. Zudem bleibt zur Not auch hier immer noch der Weg über die staatliche Repressionsschiene offen. Damit wird die Polizei mehr oder weniger zum Büttel der Vertriebsunternehmen gemacht, die profitorientiert Lücken im Sicherheitssystem bestehen lassen. Darüber hinaus bezahlt die Gesellschaft, der Bürger und Steuerzahler also, die Nachlässigkeiten der Firmen unverhältnismäßig kostenintensiv. In Relation zu dem Ermittlungsaufwand und den daraus resultierenden Verfahrenskosten wäre die Beseitigung der meisten Schwachstellen im Kontrollverfahren der Geschäftsabwicklung zur Minimierung der Tatgelegenheiten aus der „Portokasse“ zu bezahlen. Solange die Unternehmen jedoch nur die eigenen Verluste gegenrechnen (müssen), geht zumindest ihre Rechnung auf.

Das betrifft im Übrigen nicht nur die Internetkriminalität, sondern das gesamte Spektrum der Betrugsdelikte. Die Anzahl der erforderlichen Betrugskommissariate und deren Mitarbeiter steigt kontinuierlich (Tankbetrug, Warenbestell-
schwindel, Kreditkartenbetrug, Anlagebetrug, Provisionsbetrug etc.). Da wäre dann auch einmal die Frage zu stellen, ob es sich die Polizei überhaupt erlauben soll, gar darf, andere Deliktfelder wie z.B. Raub, Körperverletzung, Einbruch, Brand oder Kinder- und Sexualdelikte zu Gunsten der erdrückenden Vorgangsflut auf dem Betrugssektor zu vernachlässigen?!

Was im engeren Sinne unter dem Begriff Internetkriminalität zu subsumieren ist, wird nicht klar definiert. Die Computerkriminalität und das Themenfeld Informations- und Kommunikationstechnik (IuK-Delikte) gehören einerseits dazu, sprengen aber zugleich den eigentlichen Kernbereich Internet, der präziser als „Kriminalität in Datennetzen“ bezeichnet werden kann. Bundesweit verzeichnet die Polizeiliche Kriminalitätsstatistik (PKS) für das Jahr 2003 knapp 60.000 Fälle der Computerkriminalität. Etwa 2,5% davon betreffen das Internet. Derzeit ist das Gros der Verfahren noch der Rubrik Pornografie/ Kinderpornografie zuzurechnen, die Anzeigen im Zusammenhang mit Betrugshandlungen bei Online-Auktionen laufen den tradierten Aktionsfeldern aber zunehmend den Rang ab. Die fortschreitende Attraktivität dieser Verkaufsform lässt immer mehr im Umgang mit diesem Medium sowie dessen eigenen Regeln und Verfahrensabläufen unerfahrene User zu Opfern werden. Das Dunkelfeld dürfte beachtlich sein.
Was macht denn nun eigentlich das Internet für den Täter so attraktiv?
Zunächst die Anonymität, der er sich bedienen und zumeist gewiss sein kann. Er muss weder am Tatort auftreten noch zwingt ihn jemand, gesicherte Daten zur Identifizierung seiner Person preiszugeben. Die Nutzung von Fremdstationen, Verwendung von Nickname oder Fakeaccounts sind nur einige Tarnstrategien. So hinterlässt der Täter zwar Spuren, die führen aber oft in das Nirvana des Chat oder – wie Ermittler mitunter frustriert feststellen – in das „WORLD WIDE WEG“, wo auch regelmäßig größere Summen transferierter Gelder zu finden sind, oder gerade eben

nicht mehr.

Eine nicht unerhebliche Rolle spielt auch, dass der Täter das Opfer weder kennt noch kennen lernen muss und er dieses im Normalfall nie zu sehen bekommt. Alles läuft elektronisch und anonym ab. Ein Vorgang, bei dem es der Überwindung einer Hemmschwelle – sofern überhaupt vorhanden – kaum bedarf. Die Tatbegehung ist real zu jeder Tages- und Nachtzeit weltweit möglich. Auf Tatgelegenheiten muss nicht erst gewartet werden, die kann man sich problemlos in das Wohnzimmer klicken. Die Anzahl der verheißungsvollen Angebote für die ebenso unerfahrenen wie oft erfolgs- bzw. geldgierigen User gibt jedem von ihnen ausreichend Gelegenheit, sein Lehrgeld zu zahlen. Die immer häufiger festzustellende weitreichende Automatisierung der Geschäftswelt, der elektronischen Datenverarbeitung und Interaktion erweitert die Spielwiese krimineller Subjekte auf diesem Gebiet zunehmend. Hier bieten u.a. „Online-Banking“ oder auch „Electronic Commerce“ eine lohnenswerte Plattform, um beispielsweise Viren oder Trojaner zu implementieren und damit unrechtmäßig ggf. kostenintensive Manipulationen zu starten. Resümierend ist zu konstatieren, dass ein lückenhaftes Sicherheitssystem einerseits und das oft wenig ausgeprägte Sicherheitsbewusstsein andererseits den Schmarotzern, Parasiten, Betrügern und sonstigen Straftätern im Internet Tür und Tor öffnen.

Vieles ist – teilweise auch gesetzlich – noch nicht geregelt, also ungeklärt. Das gilt für Verfahrensabläufe, Vertragsrechte, Garantien, Ansprüche, Verpflichtungen, Zahlungsmodalitäten, Haftungsfragen, Unterverträge, Kompetenzprobleme, Kryptografie, De-Anonymisierung, Dialer-Verfahren etc.; erst nach und nach greifen Rechtsprechungen, die mitunter nur über langwierige Prozesse Klarheit und Rechtssicherheit brachten. Noch herrscht die Ellenbogenmentalität, Skrupellosigkeit und Geldgier, durchmischt in den Grauzonen des Cyberspace mit Pfiffigkeit, Cleverness und Mut, oft auch den der Verzweiflung oder Verblendung, vor. Also: Weitgehende Normen- und Regellosigkeit. Moment, das kommt uns doch irgendwie bekannt vor...

Genau, die Anomietheorie von Durkheim (Die Regeln der sozialen Methode, 2.Aufl. Neuwied 1965, 1. franz.Aufl. Paris 1895, Le suicide, Paris 1897, deutsch: Selbstmord, Neuwied, Berlin, 1967) oder Merton (Anomie, Anomia, and Social Interaction: Contexts of Deviant Behavior, New York, 1964 sowie Social theory and social structure, New York, London 1968)! Der Begriff Anomie wurde erstmalig im 16. Jahrhundert verwendet und steht für „Regel-/ Normlosigkeit“.
Ob man das Internet tatsächlich mit dem Zustand in Verbindung bringen kann und sollte, den **Emile Durkheim**, 1858 in Epinal/Frankreich geb., 1917 in Paris verstorben, als Professor an der Pariser Uni und Begründer der Kriminalsoziologie bei der Darstellung seiner Anomietheorie vor Augen hatte, darf getrost als strittig gelten. Durkheims Theorie stellt jedenfalls auf gesamtgesellschaftliche Zustände und Probleme ab. Bei entscheidenden Einschnitten in das Sozialgefüge einer Völkergemeinschaft – so seine These – verlieren alte Werte, Gesetze und Regeln ihre Gültigkeit und Anerkenntnis. Da neue Normen, die die aktuelle Situation allgemeinverbindlich regulieren könnten, noch nicht existieren oder verinnerlicht wurden, entsteht ein Vakuum, ein Zustand der Normlosigkeit eben. Derartige Situationen sind nach gravierenden Veränderungen zu erwarten, die exorbitante Ausmaße erreichen und sich eher plötzlich ereignen, wie etwa eine Revolution. Auch wenn das Internet revolutionäre Veränderungen gebracht hat, sind diese aber doch evolutionär gewachsen. Gleiches gilt für einen der Anlässe, die Durkheim zu seiner Theorie inspirierten, nämlich die industrielle Revolution, der ja zunächst auch erst einmal die technische Entwicklung vorausging. Der Weberaufstand hingegen war dann schon ein plötzliches Umbruchereignis. Warten wir also ab, ob es eines Tages den Aufstand der User geben wird.

Im Gegensatz dazu widmete sich **Robert King Merton**, der als amerikanischer Soziologe 1938 den Anomiebegriff wieder aufnahm, in seinem durchaus schichtspezifischen Ansatz zielgerichtet dem Individuum. Beiden ist aber gemein, dass sie die Kriminalität in der Gesellschaft (bis zu einem gewissen Grad an Quantität) für normal halten. Kriminalität ist demnach nicht nur integraler Bestandteil jeder gesunden Gesellschaft, sie ist als denkbare Antizipation der zukünftigen Moral und erster Schritt zur Fortentwicklung gleichsam nützlich und gewollt. Damit erscheint der Verbrecher nicht mehr schlechthin unsozial, also eine Art von Parasit oder als nicht assimilierbarer Fremdkörper im Sozialge-füge, sondern als regulärer Wirkungs-faktor.

Nach Merton definiert die Gesellschaft erstrebenswerte Ziele, die „von allen“ erreicht werden wollen. Sie gibt gleicher-maßen Mittel vor, wie diese Wünsche erfüllbar werden, nämlich durch den Einsatz legitimierter Handlungsalternativen (Arbeit, Erbschaft, Lottogewinn, Geschenke

usw.). Da die Mittel jedoch je nach Schichtzugehörigkeit und Anspruchsniveau höchst unterschiedlich sind, entsteht für denjenigen, der mit seinen ihm zur Verfügung stehenden Möglichkeiten den eigenen Ansprüchen nicht genügen, die internalisierten Ziele also nicht erreichen kann, ein anomischer Druck. Dieser muss kompensiert werden, durch Alternativstrategien zur individuellen Anpassung. Das ist möglich über fünf verschiedene Verfahrensmuster, die Merton wie folgt bezeichnet:

- Konformität
- Innovation
- Ritualismus
- Apathie/Rückzug
- Rebellion

Und genau diese fünf Typen lassen sich im Umgang mit dem Internet wiederfinden.

Konformität – sicherlich der für den Kriminologen am wenigsten ergiebige Fall – ist gegeben, wenn die Person sowohl die kulturellen Ziele als auch die institutionalisierten Mittel zur Zielerreichung anerkennt. Der also, der brav im Internet stundenlang nach Angeboten sucht und ehrliche Geschäfte abschließt.

Bei der **Innovation** werden zwar die Ziele akzeptiert, nicht aber die (ohnehin nicht ausreichenden, nicht zur Verfügung stehenden) Mittel. Durch Anwendung noch nicht anerkannter oder gar illegitimer Mittel erreicht der Delinquent sein Ziel (Besitz, Reichtum) schließlich doch. Jedes Mittel ist sozusagen recht, der Zweck „heiligt“ die Mittel. Ob ebay- Betrug, Dialerstrategien, unlautere Werbung, verbotenes Glücksspiel, Urheberrechtsverletzungen, Verstöße gegen das Arzneimittelgesetz, Vertrieb von Pornografie/Kinderpornografie, Hehlerei, Missbrach von Kreditkarten, Hacker, Phreaking (missbräuchliche Benutzung von Telekommunikationsanlagen) usw., spielt keine Rolle, Hauptsache: Innovation, also die Entwicklung neuer Ideen, die Profit bringen.

Ritualismus lehnt die Ziele ab, akzeptiert aber die ihm offenen Mittel. Die Ziele werden einfach neu definiert, herabgesetzt, während die Normen sogar überbetont und akribisch eingehalten werden (Bürokratismus etwa).

Apathie/Rückzug bedeutet Ablehnung der kulturellen Ziele und der vorgegebenen Mittel. Die Flucht aus der Realität sozusagen, z.B. in Form des Alkoholismus, Drogenmissbrauchs oder des ununterbrochenen Surfens im Internet, in jeder freien Stunde, nächtelang...

Rebellion entzieht sich allen Regeln, die interessieren nämlich gar nicht. Die Ziele natürlich auch nicht. Der politische Protest erlaubt alles, was im Sinne der
Sache zu sein scheint. Nur die revolu-tionäre Sozialstruktur wird angestrebt. Hier findet sich der Cyber-Terrorismus wieder.

Fazit: Immer mehr Menschen begeben sich freiwillig in das Internet. Sie sind guten Glaubens, dieses Netz jederzeit problemlos und unbeschadet wieder verlassen zu können, ohne zu merken, dass unliebsame Zeitgenossen die Maschen womöglich illegal bereits sehr viel enger geknüpft haben. Wer das schließlich mitbekommt und dieser Situation zu entkommen sucht, ist gezwungen, auch durch Maschen zu schlüpfen, die sich als zu klein erweisen. Dabei gehen mitunter einige Schuppen verlustig. Vielleicht behauptet daher der Volksmund, dass eine im Portemonnaie aufbewahrte Fischschuppe Geldsegen verheißen würde...

© Verlag Deutsche Polizeiliteratur