DEUTSCHER PRÄVENTIONSTAG

International Cybercrime: Results from the Annual International Forum

Jürgen Stock

Aus: Erich Marks & Wiebke Steffen (Hrsg.):
Neue Medienwelten -
Herausforderungen für die Kriminalprävention?
Ausgewählte Beiträge des 16. Deutschen Präventionstages
Forum Verlag Godesberg GmbH 2013, Seite 331-338

ISBN 978-3-942865-04-3

Jürgen Stock

International Cybercrime: Results from the Annual International Forum[1]

Ziel dieses Beitrag ist es, zu den Erkenntnissen und Ergebnissen des 5. Annual International Forum unter dem Titel "International Cybercrime Occurrence Development and Prevention" im Rahmen des 16. Deutschen Präventionstages in Oldenburg zu berichten. Das zweitägige Forum zeichnete sich durch höchst aktuelle, interessante Vorträge und Diskussionen sowie einen intensiven Austausch der anwesenden Experten aus.

Insgesamt sechs Vorträge im Rahmen des zweitägigen Forums konnten erste Antworten zu folgenden Fragen geben:

1. Wie stellt sich die aktuelle Lage des Phänomens Cybercrime dar?
2. Welche Trends und Entwicklungen zeichnen sich ab?
3. Welche Gegenmaßnahmen müssen getroffen werden, um Cybercrime effektiv zu bekämpfen?

So vielfältig sich das Phänomen Cybercrime zeigt, so unterschiedlich waren die Blickwinkel, aus denen das Phänomen beleuchtet wurde. Den Experten ist es gelungen, sozialwissenschaftliche, rechtliche, wirtschaftliche und kriminalwissenschaftliche Aspekte darzustellen.

Die Perspektive der Sicherheitsbehörden vertraten zwei Mitarbeiter des Bundeskriminalamtes, Helmut Ujen und Mirko Manske. Sie skizzierten die kriminalistische Phänomenologie, soweit diese im BKA wahrgenommen wird.

Frank Ackermann vom Eco-Verband der Deutschen Internetindustrie hat uns mit Blick auf Bekämpfungsmaßnahmen und die Kooperation der Wirtschaft mit Sicherheitsbehörden interessante Ansätze der Wirtschaft vermittelt. Der Media-Consultant Frank Tentler informierte zu Strukturen und Funktionsweisen sozialer Netzwerke, möglichen Gefahren sowie zu erwartenden Entwicklungen in diesem Bereich.

Aus der Perspektive der EU-Kommission, der politischen Ebene, legte Marc Arno Hartwig Möglichkeiten von Gegenmaßnahmen angesichts der geschilderten Gefahren dar. Abschließend berichteten Cornelia Schild vom Bundesamt für Sicherheit in der Informationstechnik und Sven Karge vom Eco-Verband von einem erfolgreich gestarteten Public Private Partnership im Bereich der Bekämpfung von Botnetzen.

---

[1] Geringfügig überarbeitete Version des am 31.05.11 in Oldenburg gehaltenen Vortrags.

„Sich im Internet bewegen ist so ähnlich wie Schlittschuhlaufen auf Natureis: Manchmal weiß man nicht, wie dünn bzw. dick das Eis ist. An manchen Stellen ist das Eis dünn und Schlittschuhlaufen gefährlich, Spaß macht Schlittschuhlaufen dennoch." Mit dieser Aussage beschrieb ein Teilnehmer sehr treffend Reiz und Risiken des Internets.

Das Internet ist ein Motor gesellschaftlicher und wirtschaftlicher Entwicklung, es ist ein Medium, das vernetzt, beschleunigt und vereinfacht. Für eine Vielzahl tagtäglicher Abläufe ist es mittlerweile unverzichtbar. Gleichzeitig müssen wir uns der Gefahren, wie sie von technischen Störungen und Cyberkriminalität ausgehen, bewusst sein. Mit den Möglichkeiten der digitalen Welt, wachsen auch die ihr innewohnenden Gefahren.

1. Lage

1.1. Positive Aspekte des Internet – soziale und wirtschaftliche Potentiale

Das Internet bietet ein enormes Potential für soziale und wirtschaftliche Entwicklungen auf nationaler und internationaler Ebene. Immer mehr Menschen haben in Deutschland Zugang zum Internet, wobei nicht nur die Jüngeren an dieser Entwicklung teilhaben, auch die Älteren, das heißt die über 60-Jährigen bewegen sich immerhin zu fast 40 % regelmäßig im Internet.[2]

Das Internet ist, da besteht keinerlei Zweifel, ein wichtiges Element der heutigen Gesellschaft: Aus Beruf, Bildung, Handel, Dienstleistung, aber auch sozialen Kontakten und hier insbesondere sozialen Netzwerken ist es nicht mehr wegzudenken. Wir alle nutzen das Internet für Prozesse wie Online-Banking, die Steuererklärung, die beim Finanzamt bevorzugt per Internet abgegeben wird, die Kfz-Anmeldung und dergleichen mehr. Durch die Mobilität der hierfür notwendigen Geräte, nicht zuletzt durch die zunehmende Verbreitung von Smartphones, kann das Internet von nahezu allen Orten, zu jeder Zeit genutzt werden. Das heißt: Der Zugang zum World Wide Web ist überall möglich, eine Bindung beispielsweise an Öffnungszeiten entfällt.

Neue Kommunikationsformen können heutzutage leicht etabliert werden; das Knüpfen und Halten von Kontakten wird zumindest technisch immer einfacher. Bei diesen Entwicklungen handelt es sich um weltweite Entwicklungen. Sie alle kennen Schaubilder, die den Anteil der Internetnutzer an der Bevölkerung in den einzelnen Ländern der Welt zeigen. Europa und die USA erscheinen dabei sehr hell, die Nutzung des Internets ist hier weit verbreitet. Doch auch auf dem afrikanischen Kontinent nimmt die Zahl der Nutzer deutlich zu.

Das ist die „helle Seite" des Internet, die Facette, die uns das Leben vereinfacht und Spaß macht.

---

[2] Bundesverband Digitale Wirtschaft: Im dritten Quartal 2010 waren 73,4% der deutschsprachigen Wohnbevölkerung in Deutschland ab 14 Jahren im Netz. Die 14- bis 39-Jährigen sind mit Anteilen deutlich über 90% nahezu vollständig im Internet präsent, bei den 40- bis 49-Jährigen sind es 86,3%, bei den 50- bis 59-Jährigen sind es 73,2%, bei den über 60-Jährigen mit 36,2% noch mehr als ein Drittel.

1.2. Gefahren des Internet – Die polizeiliche Lage

Der Schwerpunkt der Diskussionen im Forum lag jedoch auf der „dunklen Seite" des Internet, den, wie es ein Teilnehmer nannte, „Portalen der Bedrohung". Gefahren drohen in allen Bereichen: Soziale Medien, Online-Banking, Geodaten, e-Commerce. IT-Sicherheit ist häufig, so konstatierten die Referenten, nicht Teil der Ursprungsarchitektur, sondern muss zu einem späteren Zeitpunkt aufwendig und teuer nachgerüstet werden.

Cybercrime umfasst zum Teil klassische Deliktsformen, die sich lediglich im Internet duplizieren. Das Internet ist zum einen also ein neues Tatmittel. Zum anderen haben wir es mit neuartigen Kriminalitätsphänomenen zu tun, die es bisher in dieser Form nicht gab. Von den Experten wurde insbesondere der fehlende Überblick zu diesen neuen Phänomenen beklagt.

In diesem Zusammenhang ist nach Meinung der Experten fraglich, inwieweit die durch die polizeiliche Kriminalstatistik ausgewiesenen Zahlen valide sind. Stehen hinter den Zahlen möglicherweise Wirtschaftsunternehmen mit ihren spezifischen Interessen? Wie hoch ist die Dunkelziffer einzuschätzen? Die Experten des Forums äußerten hinsichtlich der Nutzbarkeit dieser kriminalstatistischen Daten Skepsis.

Cybercrime ist in der polizeilichen Kriminalstatistik einer der Wachstumsbereiche der Kriminalität. In vielen anderen Bereichen, auch bei der Zahl der Straftaten insgesamt, verzeichnen wir rückläufige Zahlen. Die Steigerungsrate im Bereich Cybercrime beträgt dagegen allein zwischen 2009 und 2010 rund 20 %. Auch hinsichtlich der durch Cybercrime verursachten Schäden sind Anstiege mit zum Teil 50 % - 60 % festzustellen. Das sind besorgniserregende Zahlen.

Bei den geschilderten Zahlen handelt es sich jedoch allein um das Hellfeld. Wie viele Delikte landen nicht bei den Strafverfolgungsbehörden, etwa weil private Geschädigte es gar nicht merken, dass ihr Rechner mittlerweile Teil eines weltweit agierenden Botnetzes ist? Wie groß ist die Zahl der Unternehmen, die einen Angriff zwar bemerken, aber aus Angst vor Imageschäden davon absehen, bei den Strafverfolgungsbehörden Strafanzeige zu erstatten?

Fest steht: Die Täter 2.0 kommen aus allen klassischen Deliktsbereichen, die polizeilicherseits und justiziell bekannt sind. Es handelt sich um Straftaten der Organisierten Kriminalität, des Terrorismus, Kinderpornografie, Wirtschaftsspionage, Betrug, bis hin zu Staatsschutz- und, Korruptionsdelikten. Im Internet findet sich alles wieder – neu sind allerdings einige Facetten, die auch die Teilnehmerinnen und Teilnehmer des Forums nachdenklich stimmten. Phänomene wie der Diebstahl digitaler Identitäten, mit denen die Täter im World Wide Web auf Einkaufstour gehen und erhebliche Schäden anrichten können, sind bedrohlich. Auch die Möglichkeit der Erstellung von digitalen Klonen, sozusagen von Parallel-Identitäten, weist ein enormes Schadenspotential auf.

Das gilt auch für die Entwicklungen im Bereich Pishing. Sie alle kennen dieses Phänomen, viele haben schon einmal so genannte Phishing-Mails erhalten: Was vor ein paar Jahren noch relativ plump anfing, ist mittlerweile durch entsprechendes Social Engineering der Täter professioneller geworden. Trojaner fängt man sich heute durch sog. „Drive-by-Infection" ein. Bei einer vermeintlich nicht kompromittierten Webseite, wie beispielsweise der Webseite des Bundeskriminalamtes oder des Bundesamtes für Sicherheit und Informationstechnik, könnte es sich um eine – kaum von der echten zu unterscheidende – gefälschte Seite handeln, über die beim Abrufen der Inhalte ein Trojaner auf den eigenen Rechner gespielt wird.

Auch klassische Deliktsbereiche wie Erpressung, Schutzgelderpressung, Lösegelderpressung, spielen sich heute im Internet ab. Es gibt, wenn wir den Terminus fortführen, eine Mafia 2.0, die nicht mehr irgendwo eine Bank überfällt, sondern heute mit den Möglichkeiten des Internet auf Unternehmen zugeht und diese mit Spam-Attacken bedroht. Wenn die derart bedrohten Unternehmen die Drohungen nicht ernst nehmen, werden die Server überlastet. Die Nicht-Erreichbarkeit der Unternehmen aufgrund der Überlastung ihrer Server kann erhebliche Verluste verursachen. Entsprechende Fälle haben gezeigt, dass hinter der Bedrohung ein realer Schaden steht, der ein Unternehmen, manchmal sogar kleinere Staaten, vor erhebliche Probleme stellen kann.

Ein Thema der Zukunft, darauf haben die Experten nachdrücklich hingewiesen, sind mobile Endgeräte. Viele Menschen verfügen bereits über solche Endgeräte, die immer mehr Funktionen in sich vereinen. Die Konsequenz ist, dass mobile Endgeräte in Zukunft vermehrt Ziel von Attacken beispielsweise durch Botnetze sein werden. Dies ist sicherlich ein Bereich, der unter Präventionsgesichtspunkten in Zukunft im Focus stehen sollte.

Inzwischen hat sich eine Underground Economy entwickelt, eine breitgefächerte Produkt-Palette krimineller Angebote im Netz. Mit relativ geringem finanziellen Aufwand können digitale Identitäten, Kreditkartendaten, Trojaner oder ganze Botnetze erworben und auf dieser Basis mit relativ begrenzten IT-Kenntnissen erhebliche Schäden angerichtet werden.

Mit der Formulierung „That has been our depression day" beschrieb ein Teilnehmer treffend den ersten Tag des 5. Annual International Forum. Was kann oder muss im Bereich der Prävention gemacht werden, greifen die Instrumente, die wir haben? Wo können wir ansetzen, wenn der eigene Rechner zu einer potenziellen Bedrohung werden kann? Dies waren die Fragen, mit denen wir in den zweiten Tag starteten.

2. Gegenmaßnahmen – Akteure und Methoden

Im Mittelpunkt der Diskussionen zu Akteuren und Methoden von Gegenmaßnahmen standen die Fragen: Welche Gegenmaßnahmen im Bereich der Prävention können wir anbieten? Welche Akteure und Methoden sind bislang involviert? Nahezu alle Refe-

renten waren der Auffassung – und dies ist meines Erachtens eine wichtige Botschaft, die von dem diesjährigen Präventionstag ausgeht – dass wir uns einerseits national und international über eine große Zahl verschiedenster Initiativen freuen können. In der Entwicklung von Gegenmaßnahmen gegen Cybercrime sind viele Akteure sehr engagiert. Es gibt jedoch auch Bereiche, in denen von den Experten noch erheblicher Aufholbedarf gesehen wird. So müssen wir beispielsweise im Bereich „Awareness", also der technologischen und bewußtseinsbezogenen IT-Sicherheit, schleunigst Gegenmaßnahmen ergreifen. Die Schere zwischen der Entwicklung im Bereich Cybercrime und dem, was wir dieser Entwicklung entgegensetzen, darf nicht noch weiter auseinandergehen.

2.1. Sicherheitsbehörden

Seit März dieses Jahres verfolgt die Bundesregierung eine gemeinsame Cyber-Sicherheitsstrategie. Die Sicherheitsbehörden übernehmen dabei ihre klassischen Aufgaben der Strafverfolgung und Gefahrenabwehr. Mitarbeiter aus verschiedenen Arbeitsfeldern, wie Wissenschaftler, Techniker, Polizisten und andere Experten arbeiten in den Sicherheitsbehörden tagtäglich zusammen. Im Bereich der klassischen polizeilichen Repression steht die Polizei und auch die Justiz unter anderem vor der Herausforderung, Lösungen zu finden, wie Spuren im Netz so gesichert werden können, dass sie hinterher im Strafprozess verwertbar sind. Eine weitere Herausforderung sind die großen Datenmengen, die es im Zuge von Ermittlungsverfahren auszuwerten gilt.

Die Experten im Forum wiesen auf die Notwendigkeit hin, sich intensiv mit künftig zu erwartenden Entwicklungen zu befassen. Aufgrund der der Cybercrime inhärenten Dynamik sind wir gut beraten, mit Methoden wie der Szenariotechnik zu verfolgen, welche künftigen Entwicklungen zu erwarten sind. Hierzu gehört auch, ein funktionierendes Monitoring zu betreiben. Vom beklagten „Hinterher-hecheln" müssen wir zum „Vorausschauend-tätig-werden" kommen. Beispiele neuerer Entwicklungen sind moderne Bezahlsysteme, wie Web-Money oder U-Cash, wobei auch eher (noch) futuristisch anmutende Themen wie in der Entwicklung begriffene „digitale Tarnkappen", mit denen man kriminelles Tun verschleiern kann, von den Experten vorgestellt wurden.

2.2. Wirtschaft und Verbände

Wirtschaft und Verbände wiesen auf die verschiedenen Plattformen und Kooperationsformen, die zur Prävention bislang etabliert sind, hin. Hierbei handelt es sich zum einen um Aktivitäten der Wirtschaft auf ihren eigenen Aktionsfelder, zum anderen sind Beispiele genannt worden, in denen Präventionsprogramme anderer Akteure, etwa von Schulen insbesondere im kommunalen Bereich, von Wirtschaftsunternehmen und Verbänden unterstützt werden.

2.3. User/Nutzer

Auch der Nutzer selbst ist gefragt und muss sich als zentrales Element der Sicherheitsstruktur verstehen. Die „Awareness", die Sensibilität gegenüber den Gefahren des Internet muss gestärkt werden. Vor dem Hintergrund, dass auch eine installierte Antiviren-Software keine hundertprozentige Sicherheit bietet, sondern immer nur einen Teil der aktuell auf dem Markt befindlichen Viren identifizieren kann, kommt dem Nutzer eine besondere Verantwortung zu.

2.4. Privat-Public-Partnership

Das Thema Public Private Partnership wurde anhand eines aktuellen Beispiels, dem Anti-Botnetz-Beratungszentrum, vorgestellt. Das Anti-Botnetz-Beratungszentrum ist eine Kooperation zwischen BSI (Bundesamt für Sicherheit und Informationstechnik) und dem Eco-Verband. In diese enge Kooperation sind auch Internet-Service-Provider und Hersteller von Anti-Viren-Software eingebunden. Das Bemerkenswerte an diesem Konzept ist, dass es sich nicht nur um ein strategisches Beratungsgremium handelt, sondern den von einer Botnetz-Attacke betroffenen Unternehmen ebenso wie Einzelpersonen eine konkrete Beratung angeboten wird. Die Experten versicherten, zur Not gingen die Mitarbeiter des Callcenter mit dem Anrufer Punkt für Punkt einen Arbeitsplan durch, um am Ende den für die Einbindung des Rechners in das Botnetz verantwortlichen Trojaner wieder vom Rechner zu entfernen.

3. Fazit

Wie bereits mehrfach angedeutet, bleiben in dem dynamischen Bereich der Cybercrime viele Aspekte bisher offen. Die Phänomenkenntnisse sind teilweise nicht sehr fundiert, ein Bewusstsein für die drohenden Gefahren muss gestärkt werden. Welche Schlüsse können aus den Vorträgen und Diskussionen insbesondere für die Prävention gezogen werden?

3.1. Ausbau bestehender Kooperationen

Zahlreiche Akteure sind bereits in dem Feld der Prävention von Cybercrime aktiv. Bereits bestehende Kooperationen müssen weiter ausgebaut und gestärkt werden. Gerade im Bereich der Prävention gibt es noch Optimierungspotential.

3.2. Mit der Entwicklungsdynamik Schritt halten

Die Entwicklungsdynamik des Internet und damit auch der Cybercrime wird sich nach Auffassung der Experten nicht abschwächen. Frau Prof. Potja führte treffend aus, dass früher bei Innovationen im Bereich der Technik viel Zeit blieb, um über Problemlösungen nachzudenken. Die Experten im Forum waren sich einig, dass diese Zeit heute nicht mehr zur Verfügung steht. Wir müssen schneller reagieren und verstärkt präventiv tätig werden.

3.3. Stärkung der Forschungsaktivitäten

Forschungsaktivitäten im Bereich Cybercrime müssen forciert werden. Die Phänomenologiekenntnisse zu dem, was im Internet passiert, sind auszuweiten. Es ist ein Aufgabenfeld der klassischen Kriminologie, mehr über Erscheinungsformen und das quantitative Ausmaß von Cybercrime zu erfahren. Auch die Aufhellung des Dunkelfelds zählt zur klassischen sozialwissenschaftlichen Forschung und ist ein Bereich, der angegangen werden muss. Auf der anderen Seite ist die technologiebezogene Forschung zu Vermeidung von Tatgelegenheiten im Internet, insbesondere zur IT-Sicherheit zu verbessern. Nur so können wir nähere Erkenntnisse zu Risiken sowie Tat-, Opfer- und Täterstrukturen erlangen.

3.4. Bekämpfung des Cybercrime als gesamtgesellschaftliche Aufgabe

Die Bekämpfung von Cybercrime ist eine gesamtgesellschaftliche Aufgabe. Mit ihren Vorträgen verdeutlichten die Experten, dass Cybercrime ein klassisches Querschnittsthema ist. In der Konsequenz heißt das: Wir müssen ressortübergreifende Strategien entwickeln, jeder muss seinen Teil der Verantwortung in der präventiven Wertschöpfungskette vom privaten User über Unternehmen und über staatliche Akteure annehmen.

3.5. Intensivierung des gesellschaftlichen Diskurses

Der gesellschaftliche Diskurs über das Internet, was dort passieren soll und was dort nicht passieren soll, muss nach Auffassung der Experten intensiver geführt werden.

„Don‘t be stupid“, das ist die simple Formel der Prävention. Aber ist das ausreichend oder benötigen wir mehr Reglementierung? Welches Maß an Freiheit soll es im Netz geben? Welche Rolle kommt den einzelnen Akteuren zu? Reicht eine reine Netzethik, die sozusagen von den Usern selbst entwickelt wird oder brauchen wir mehr staatliche Regulierung? Das World Wide Web ist einerseits weltumspannend. Doch bereits der Blick auf die europäischen Staaten zeigt, die Bewertung, inwieweit der Staat eingreifen sollte, fällt zum Teil höchst unterschiedlich aus. Die Diskussion über das Zugangserschwerungsgesetz, das in Deutschland eingeführt und wieder aufgehoben wurde, verdeutlicht exemplarisch die Problematik.

3.6. Stärkung der Medienkompetenz

Die Medienkompetenz muss im Sinne eines universellen Präventionsansatzes quer durch die Gesellschaft weiter ausgebaut und gefördert werden. Aufklärung und Prävention muss bei Kindern in dem Moment beginnen, in dem sie das erste Mal ein Gerät in die Hand nehmen, das mit dem Internet verbunden ist. In diesem Moment muss spezifische Erziehung und Awareness-Produktion ansetzen.

3.7. Neue Kooperationsformen zwischen privaten und öffentlichen Akteuren

Wir müssen neue Kooperationsformen zwischen privaten und öffentlichen Akteuren erproben, auf nationaler wie auf internationaler Ebene. Es gibt lokal, national, international eine Menge an bereits bestehenden oder sich derzeit entwickelnden Kooperationsformen. Diese müssen weiter erprobt und ausgebaut und nach Möglichkeit in einigen Fällen auch wissenschaftlich begleitet werden, damit wir definieren können, wie diese Netzwerke effektiv zu organisieren sind.

3.8. Ausbau individueller Hilfsangebote

Nach Überzeugung der Experten müssen die individuellen Hilfsangebote ausgebaut werden. Das Botnetz-Beratungszentrum als gemeinsame Aktion einer Behörde und eines Verbandes ist ein gutes Beispiel hierfür. Es wurde im Forum mit der polizeilichen Einbruchsberatung verglichen. Das heißt klassische Kriminalitätsfelder, in denen die Polizei einen großen Beratungsapparat aufgebaut hat, müssen, so die Experten, auf den Bereich Cybercrime ausgeweitet werden. Es bedarf einer staatlichen Stelle, bei der man anrufen und sich beraten lassen kann.

3.9. Anpassung der Präventionsmethodik

Unsere Präventionsmethodik muss angepasst werden. Die Präventionsakteure brauchen ein neues spezifisches Social Engineering, sie müssen wissen, wie sie die entsprechenden Zielgruppen erreichen. „Listen, Learn and Lead“ sind die Schlagworte – also zuhören, lernen und am Ende die Führung im Sinne von Präventionsaktivitäten übernehmen. Insoweit haben wir einen Punkt des Beitrages von Wiebke Steffen gestern etwas in Frage gestellt: Ob die Methoden der analogen Welt auf die digitale übertragbar sind. Nach dem Ergebnis unseres Forums ist das fraglich, was in der Konsequenz bedeutet, dass ein spezifisches Instrumentarium entwickelt werden muss.

3.10. Zurverfügungstellung von Ressourcen

Für Gegenmaßnahmen und Prävention müssen genügend Ressourcen zur Verfügung gestellt werden. Das ist nicht überraschend, letztlich ist es einer der angenehmen Nebeneffekte von Public Private Partnership, dass die Wirtschaft sich finanziell mit engagiert und gemeinsam Kooperationen auf die Beine gestellt werden, mit Hilfe derer Trainings und Schulungsmaßnahmen finanziert werden können.

Soweit die wesentlichen Erkenntnisse aus dem 5. Annual International Forum des 16. Deutschen Präventionstages.

Ich will die Gelegenheit nutzen, von dieser Stelle aus allen Referenten herzlich für die sehr guten Vorträge und den Diskutanten für die Beiträge in den Diskussionsrunden zu danken. Vielen Dank für ein informatives und zielorientiertes Forum.

Inhalt