



**Tatort Internet: Kriminelle knacken heutzutage nicht mehr Panzerschränke, um zu Geld zu kommen, sondern sie hacken und plündern Konten.**

## Tatort Internet

**Bei einer Fachtagung des Bundes Deutscher Kriminalbeamter am 4. und 5. Mai 2010 in Leipzig wurden Wege zur Bekämpfung der Internetkriminalität aufgezeigt.**

Das Internet hat sich zum größten Tatort entwickelt“, sagte der sächsische Staatsminister des Innern, Markus Ulbig, bei der Eröffnung der vom Bund Deutscher Kriminalbeamter in der Messe Leipzig im Rahmen der GPEC veranstalteten Fachtagung „Tatort Internet“. Um zu Geld zu kommen, würden heutzutage nicht mehr Panzerschränke geknackt, sondern Konten gehackt und geplündert. Über das Internet würden gezielte Angriffe auf Unternehmen und Regierungen durchgeführt, über soziale Netzwerke würden Opfer gesucht, Menschen zu Terroristen ausgebildet und Anleitungen zum Selbstmord gegeben. Viel zu wenig werde bedacht, dass eine Milliarde Menschen eine über das Internet verbreitete Nachricht lesen können. Viel zu sorglos werde mit Daten umgegangen. Vor allem Kinder und Jugend-

liche müssten auf diese Problematik hingewiesen werden.

„Während die Polizei noch mit Pfeil und Bogen kämpft, führen Kriminelle bereits das Laserschwert“, umriss Richard Benda, Präsident der „Vereinigung Kriminaldienst Österreich“, als Gastredner bei der Eröffnung der Veranstaltung das Problem bei der Verfol-

gung von im oder über das Internet begangenen Straftaten. Die Tagung sollte demgemäß auch den Anstoß zu neuen Initiativen geben, betonte der Präsident des *Bundes Deutscher Kriminalbeamter*, Klaus Jansen.

**Über Botnetze** und die von ihnen ausgehenden Gefahren referierte Prof. Dr. Peter Martini von der Universität Bonn. Schadprogramme suchen sich selbstständig Rechner, die Sicherheitslücken aufweisen, nisten sich über die Schwachstelle ein – bereit, ferngesteuert und koordiniert etwa andere Rechner lahmzulegen (DDoS-Attacken) oder Spam zu versenden. Angriffe durch mehrere Hundert Rechner reichen bereits aus, einen angegriffenen Rechner zu „fluten“. Um Gegenmaßnahmen ergreifen zu können, werden derartige Schadprogramme in „Honeypots“ auf-



**Peter Martini:**  
„Schadprogramme suchen sich Rechner selbstständig.“



**Axel Henrichs:**  
„Soziale Netze auch für Polizei zugänglich sein.“

gefangen und analysiert. Hat es bis vor wenigen Jahren noch gereicht, die Kommandozentrale auszuschalten, hat sich mittlerweile eine „Peer-to-Peer“-Technologie entwickelt: Jeder infizierte Rechner stellt bereits für sich einen Kommando- und Kontrollserver (C&C-Server) dar und es müsste somit jeder einzelne davon aus dem Netz genommen werden.

Die wirksamste Gegenmaßnahme, einen „Gegenwurm“ einzusetzen, der auf dem gleichen Verbreitungsweg von sich aus die Schadprogramme unschädlich macht, scheitert daran, dass nach geltender Rechtslage ohne Zustimmung des Berechtigten – in diesem Fall eben des Verbreiters der Malware – Programme nicht verändert werden dürfen. Nicht einmal der IP-Service-Betreiber, der erkannt hat, dass an seinem Netz ein infizierter Rechner hängt, darf diesen aus dem Verkehr ziehen, sondern kann den Betreiber dieses Rechners lediglich darauf hinweisen und auffordern, Maßnahmen zu setzen, die eine Weiterverbreitung des Schadprogramms durch ihn verhindern.

**Soziale Netzwerke.** „In Deutschland sind 30 Millionen Menschen Mitglieder von sozialen Netzwerken, allein *StudiVZ* hat 14,5 Millionen Teilnehmer“, führte Dr. Axel Henrichs von der FH für Öffentliche Verwaltung Mainz aus. „Was für jedermann zugänglich ist, muss auch der Polizei zugänglich sein können. Was spricht dagegen, die in diesen Netzen freiwillig veröffentlichten Daten auch für polizeiliche Zwecke zu nutzen?“ Da rechtliche Regelungen fehlten, wären Rechtspositionen aus der realen Welt analog in die virtuelle zu übertragen: Ein Eindringen in geschützte virtuelle Räume müsste unter denselben Voraussetzungen stattfinden sein, wie dies auch für das Eindringen in Räumlichkeiten gelte, die durch das Hausrecht geschützt sind, zumal dies weniger eingriffsintensiv sei als eine reale Hausdurchsuchung.

Henrichs warnte allerdings davor, dass Polizeibeamte auf eigene Faust unter privaten Zugängen Ermittlungen im Netz führen. Dies könnte unter anderem eine zivilrechtliche Haftung nach sich ziehen. Der Begriff des verdeckten Ermittlers müsse per Gesetz auf Ermittlungen im Netz ausgeweitet werden, wie überhaupt die polizeiliche Ermittlung bei zeitgemäßer Regelung darauf abgestellt werden müsste, dass



**Marcus Stewen:** „Einfache Nacktdarstellungen sind nicht strafbar.“



**Werner Dohr:** Täter tritt im Internet mit Identität eines anderen auf.“



**Ulrich Kleuser:** „Schnellere Ermittlungen bei Onlinedelikten.“



**Marco Thelen:** „Rechtshilfeverfahren bei Onlinedelikten zu lange.“

die Polizei „zur Erfüllung ihrer Aufgaben auch im Internet aufklären und sich insbesondere seiner Dienste bedienen darf“. Bei der Einstellung von Beamten in den Polizeidienst sollte dem Einstellungswerber eine Erklärung abverlangt werden, dass er damit einverstanden ist, dass hinsichtlich seiner Person soziale Netzwerke ausgewertet werden dürfen. Des Weiteren sollten Polizeibeamte unter anderem verpflichtet werden, sich in sozialen Netzen

nicht über ihren Dienst oder ihren Dienstgeber zu äußern. Um dennoch eine Meinungs- und Informationsplattform zu schaffen, könnte ein eigenes, nach außen abgeschottetes Kommunikationsnetz nur für Polizeibeamte in Betracht gezogen werden, in dem diese auch anonym oder unter Pseudonym auftreten können.

**Kinderpornografie im Internet.** „Der Umsatz an Kinderpornografie wird weltweit auf 3 bis 20 Milliarden US-Dollar geschätzt“, berichtete Marcus Stewen vom LKA Nordrhein-Westfalen. In der Datenbank von Interpol sind über eine Million einschlägiger Bilder gespeichert. Die Auswertung ergibt, dass diese Bilder zu 20 Prozent Kinder im Alter von 3 bis 6 Jahren betreffen, zu 45 Prozent im Alter von 7 bis 10, zu 30 Prozent zwischen 11 und 15 Jahren und nur zu 1 Prozent Jugendliche zwischen 16 und 17 Jahren. Strafrechtlich nicht relevant seien „Lookalikes“ mit volljährigen Darstellern, „Modelbilder“ mit bekleideten Kindern, einfache Darstellungen der Nacktheit etwa in Bildern von FKK-Stränden oder künstlerische Thematisierungen. Wohl aber fallen darunter „Posenfotos“ mit eindeutiger Betonung der Geschlechtsteile.

Von Bedeutung sei laut Stewen nicht die Anzahl der Bilder, die bei einem Täter vorgefunden werden, sondern in welchem zeitlichen Zusammenhang sie erworben wurden. Die abgespeicherten Bilder hätten in der Abfolge der Speicherung den Charakter eines Tagebuchs, aus dem sich die Gefährlichkeit eines Täters und die Wiederholungsfähigkeit ableiten lassen.

Mit dem Ergebnis einer KIM-Studie aus dem Jahr 2008, wonach 40 Prozent der Kinder zwischen 6 und 7 Jahren PC-Nutzer waren, im Alter von 12 und 13 bereits zu 91 Prozent, stellte die Kriminalpsychologin Petra Rump ein Präventionsprojekt gegen Kinderpornografie der Polizei Bremen vor, in dessen Rahmen auf verschiedenen Ebenen eine Bewusstseinsbildung und Sensibilisierung für dieses Thema herbeigeführt werden soll. Polizisten halten Vorträge in Schulklassen und bei Elternabenden und wirken bei der Lehrerfortbildung mit. Speziell für unter 18-Jährige geschaffene Internetforen und deren Chatforen (Beispiele dafür sind [www.knuddels.de](http://www.knuddels.de) und [www.smoodoos.com](http://www.smoodoos.com)) könnten Treffpunkte für Pädophile sein. Die Täter

**BDK**

**Standesvertretung**

Der 1968 gegründete *Bund Deutscher Kriminalbeamter (BDK)* vertritt die beruflichen und sozialen Belange aller Angehörigen der Kriminalpolizei. Er setzt sich weiters im Zusammenwirken mit den Medien und politischen Entscheidungsträgern für eine praxisnahe, realistische und fortschrittliche Kriminalitätskontrolle ein. Drei Jahre nach der Gründung wurde die erste internationale Tagung von Kriminalisten durchgeführt. Der Verein gibt die zehnmal jährlich erscheinende Fachzeitschrift „der kriminalist“ heraus.

[www.bdk.de](http://www.bdk.de), [www.kripointer.de](http://www.kripointer.de)

FOTOS: KURT HECKSCH

geben sich entweder als Kind oder als liebevoller Erwachsener aus, treten mit Nicknames wie „Taschengeld für Dich“ auf, und versuchen, mit Gesprächen über Sex, Liebe und Flirten den Kontakt zu steigern.

Als Vorsichtsmaßnahme für die Teilnahme an solchen Foren empfiehlt Rump, das Passwort geheim zu halten, einen neutralen Nicknamen zu wählen, so wenig wie möglich an persönlichen Daten preiszugeben und keine oder lediglich stilisierte Fotos ins Netz zu stellen. Auch die Webcam sollte nicht in Betrieb sein. Kinder sollten dazu angehalten werden, bei „komischen“ Situationen Screenshots anzufertigen und auf einem neben dem Rechner bereit liegenden Notizzettel Datum und Uhrzeit zu notieren und mit ihren Eltern darüber zu reden. Ein Treffen im realen Leben sollte niemals ohne Mitnahme einer Vertrauensperson erfolgen und an einem öffentlichen Ort stattfinden.

**Cybermobbing** ist ein Phänomen mit einer Multiplikatorwirkung insofern, als sich auch unzählige andere an den Äußerungen über eine Person beteiligen können. Abfällige Äußerungen über den Arbeitgeber könnten bei Polizeibeamten dienstrechtliche Folgen haben, ebenso persönliche Fotoalben, die einen dienstlichen Hintergrund haben. Rump schlug vor, die vom Beamten abzugebende Datenschutzerklärung auf das Verhalten im Internet zu erweitern.

Dass sich in Chatforen für Jugendliche abfällige Äußerungen über die Schule oder Lehrpersonen finden, mag noch angehen, wenngleich sie sich den Tatbeständen der Beleidigung, der üblen Nachrede, Nötigung, Erpressung oder Verstöße gegen Persönlichkeitsrechte annähern. Gruppen, die sich bei Einträgen über „Lehrer abknallen“ bilden, stimmen bedenklich.

**Strafverfolgung.** Wie sich I&K-Kriminalität, Straftaten, unter Ausnutzung moderner Informations- und Kommunikationstechnik, aus Sicht eines Er-



**Fachtagung „Tatort Internet“ in Leipzig: BDK-Bundesvorsitzender Klaus Jansen, Innenminister Dato Seri Hishammuddin Tun Hussein (Malaysia), Innenminister Markus Ulbig (Sachsen), VKÖ-Präsident Richard Benda.**

mittlungsbeamten darstellt, schilderte Werner Dohr vom Landeskriminalamt Nordrhein-Westfalen. Man kämpft mit der enormen Datenmenge, wenn in ein Botnetz eingedrungen werden soll, um die Kontakte und die Struktur der dahinter stehenden organisierten Kriminalität zu ermitteln. Datenmengen von 5 bis 10 GB pro Tag sind zu überwachen sowie Millionen von Datenpaketen. Bei Volllast werden pro Tag 1,25 Milliarden Phishing-Spam-Mails versendet, was immerhin 15 Prozent des weltweiten E-Mail-Aufkommens ausmacht.

Die Entwicklung geht zu „Man-in-the-Middle-Attacken“, wobei der Datenverkehr nach relevanten Informationen abgehört wird. Dazu kommt der Identitätsdiebstahl: Der Täter tritt im Internet mit der Identität eines anderen auf.

**Anbieter von „Bulletproof Hosting“** versorgen ihre Kunden mit einem Server-Standort, der „kugelsicher“ vor Zugriffen internationaler Ermittler ist. Gegenüber „Bulletproof Hosting“ können Beweismittel nur mehr dadurch gewonnen werden, dass die im Bereich der Geldwäsche, des Großbetrugs oder der sonstigen organisierten Kriminalität agierenden Täter am eingeschalteten, mit dem Server in Verbindung stehenden Rechner überrascht werden. Die Frage stellt sich laut Dohr, ob eine Online-Durchsuchung nicht doch das weniger eingriffsintensive Mittel darstellt, als ein überfallsartiges gewaltsames Eindringen in Räumlichkeiten.

„Wir müssen schneller werden“, forderte Ulrich Kleuser, Staatsanwalt beim LG Bonn. Ermittlungen zu IP-Adressen in Phishing-Fällen würden, in Anbetracht der durch Botnetze gesteuerten Rechner sorgloser Nutzer kaum zum Erfolg führen und seien weitgehend sinnlos. Tatornte ließen sich nicht mehr ausmachen. Das auf die örtliche Zuständigkeit aufgebaute System müsse in Richtung einer Konzentration überdacht werden, da die Ver-

fahren zersplittern und Fragen über die Zuständigkeit Sachfragen überdecken würden. Vollends scheitere man mit diesem System beim „Cloud Computing“, bei dem Daten und Programme „in der Wolke“, dem Internet, liegen, und nicht einmal der Anwender weiß, wo Zugriffe sind dann nur mehr bei eingeschaltetem Rechner erfolgreich. Es gibt keinen greifbaren physischen Server mehr. Für Fälle der schwerstrafbare Kriminalität müsse gesetzlich die Online-Durchsuchung ermöglicht werden. Das Urteil des Bundesverfassungsgerichts vom 2. März 2010 zur Vorratsdatenspeicherung habe Wege aufgezeigt, wie etwa die Erstellung eines Katalogs in Betracht kommender schwerer Straftaten.

Staatsanwalt Marco Thelen von der Staatsanwaltschaft Bonn bemängelte, dass die Vielzahl von Straftaten im Internet schwer zu bündeln sei und dass Rechtshilfeverfahren viel zu lange dauern würden. Zur enormen Datenflut komme die Masse von Zufallsfunden. Wenn man unter Online-Durchsuchung die Online-Durchsicht von Datenbeständen verstehe, sei diese mit den derzeit bestehenden Gesetzen tatsächlich nicht in Einklang zu bringen. Die Online-Überwachung hingegen sei als Überwachung der Telekommunikation bereits gesetzlich geregelt. Das Einstellen von Bombenbauanleitungen in das Internet ist in Deutschland nach § 91 in Verbindung mit § 89a dStGB strafbar, wenn dies eine Anleitung zur Begehung einer schweren staatsgefährdenden Gewalttat sein soll. *Kurt Hickisch*