



Grußwort

der Justizministerin Dr. Beate Merk

"Forum Cyber Crime"

am 5. Oktober 2011
im Justizpalast München

Übersicht

1. **Einführung:** Fälle zur Cyberkriminalität

2. In Bayern schon ergriffenen Maßnahmen zur Bekämpfung der Internetkriminalität:

- Mustervereinbarung StA - Polizei
- Ansprechpartner/ Sonderzuständigkeiten
- Zuständigkeitsvereinbarung
- Datenbank
- Fortbildung

3. **Erwartungen** an diese Tagung

4. **Begrüßung** der wichtigsten Referenten

Es gilt das gesprochene Wort

Anrede!

Kennen Sie den Fall der Steuerberatungskanzlei in Hessen, die Opfer von Cyberkriminellen wurde?

Die "Cracker" aus Südamerika haben ein "trojanisches Pferd" an die Kanzlei geschickt und so 12 PC des Unternehmens infiziert. Der Trojaner wurde in einem ganz gewöhnlichen pdf-Format versteckt.

Mit der digitalen Schädigung konnten die Täter die Tastatureingaben protokollieren und Bildschirmkopien, E-Mails und Dateien jeder Art auf Server in Russland übertragen.

Erst ein halbes Jahr, nachdem die Daten gesaugt worden waren, forderten die Kriminellen 100.000 Euro. Die Drohung: Falls nicht gezahlt werde, würden die Mandantendaten im Internet veröffentlicht. Das Geld sollte auf ein Konto in Argentinien überwiesen werden.

Der Grund für die Wartezeit: Die Daten waren zwar innerhalb weniger Stunden kopiert. Die Hacker hatten aber beim Zugriff auf die Daten festgestellt, dass die Kanzlei im Moment nicht ausreichend "flüssig" war und deshalb gewartet, bis wieder ausreichend Guthaben auf dem Kanzleikonto stand.

Das gleiche Bild bei einem Sondermaschinenbauer hier in Süddeutschland:

Ein Mitarbeiter des Unternehmens war geschäftlich in Hongkong. Nach den Verhandlungen dort gab es ein geschäftliches Abendessen, das auf Video festgehalten und später per Mail zur Erinnerung an den schönen Abend nach Deutschland geschickt wurde. Trojaner in der Datei inklusive!

Die Daten der Forschungs- und Entwicklungsabteilung wurden kopiert und an einen chinesischen Wettbewerber geschickt.

Der konkurriert jetzt mit Produkten um Kundenaufträge, die zu 100 % auf den kopierten Daten basieren.

Geschätzter Schaden: 5 Millionen Euro.

Anrede!

Was ich Ihnen eben geschildert habe: Das sind nur ganz wenige Beispiele von vielen.

Wer einen Internetanschluss hat, wer sich bei Google eine Anonymisierungssoftware herunterladen kann: Der kann im Internet oft genug tun und lassen, wonach ihm der Sinn steht:

- Kinderpornos ansehen.
- Anleitungen zum Bombenbau ausdrucken.
- Drogen bestellen.
- Eine Lunge, eine Niere, eine Leber kaufen.
Oder verkaufen.

- andere Identitäten klauen und diese selber nutzen oder verkaufen: auf Nutzeraccounts, bei E-Commerce und E-Government, beim Online-Banking, bei Kreditkarteninformationen
- Lügen und Betrügen. Zum Spaß oder aus Gewinnsucht. Ganz egal! Und meistens, ohne erwischt zu werden.

Deutschlandweit wurden im Jahr 2010 rund 60.000 Fälle im Bereich der Internetkriminalität angezeigt. Das ist eine Zunahme von fast 19 %.

Auch bei den registrierten Schäden ist ein großer Anstieg zu verzeichnen. Allein beim Computerbetrug beliefen sich die Schäden voriges Jahr auf 47 Millionen Euro.

Hinzu kommt - wie wir alle wissen - eine große Dunkelziffer. Diese kommt dadurch zustande, dass viele Opfer den Betrug gar nicht bemerken, weil die Schadenssumme klein ist. Viele Geschädigte erstatten auch keine Anzeige, weil sie Sorge haben, dass sie dann nicht mehr als zuverlässiger Partner im Netz oder Geschäft wahrgenommen werden würden.

Was bei der Cyberkriminalität auffällt: Nicht nur die Anzahl und Begehungsweise der Taten hat sich verändert. Auch die Täterstrukturen sind anders.

Vor einigen Jahren war Internetkriminalität das Gebiet der hoch spezialisierten Täter mit Expertenwissen.

Jetzt sind es auch genügend Alltagskriminelle, die sich die Schadsoftware für ihre Taten einfach herunterladen. Die Täter wirken dabei weltweit zusammen.

Anrede!

Wenn Sie mich fragen: Ich sehe auf dem Gebiet der Cyberkriminalität eine enorme Dynamik. Kriminalität wird sich auch in Zukunft mehr und mehr verlagern von der realen Welt auf das World Wide Web.

Wir alle sind gefordert, das ökonomische Potenzial und die soziale Sicherheit im Netz zu schützen!

Effektives Vorgehen gegen Internetkriminalität - das ist das dringende Gebot der Stunde! Es geht darum, unsere Freiheit im Netz zu erhalten - indem man das Netz schützt.

Was also ist zu tun?

Wir brauchen die rechtlichen Voraussetzungen, um Internetkriminalität bekämpfen zu können - Stichworte Vorratsdatenspeicherung, Lückenschließen beim Grooming und beim Cyber-Mobbing, Rechtshilfe und grenzübergreifende Zusammenarbeit.

Wir müssen aber auch unsere eigene Effektivität und Zusammenarbeit steigern.

Wir haben schon **Muster für Vereinbarungen** zwischen Staatsanwaltschaften und Polizei erarbeitet. So können Anzeigen, bei denen ein strafbares Handeln nicht erkennbar ist, dem Staatsanwalt in vereinfachter Form vorgelegt werden.

Bei den Staatsanwaltschaften haben wir **Ansprechpartner** benannt und **Sonderzuständigkeiten** eingerichtet, um das vorhandene Wissen zu bündeln und zu fördern.

Auf meine Initiative hin optimieren die deutschen Generalstaatsanwälte die Strafverfolgung von Massendelikten wie etwa bei Kostenfallen im Internet.

Geplant ist außerdem, bei einer zentralen Polizeidienststelle eine **Datenbank** vorzuhalten. Hier sollen alle Informationen zu Internetseiten eingestellt werden, die von einem Ermittlungsverfahren betroffenen sind.

So kann der einzelne Staatsanwalt, der über einem einzelnen kleinen Internetbetrug sitzt, prüfen, ob sein Fall nicht vielleicht nur ein kleiner Krümel aus dem großen Kuchen ist. Und welche Staatsanwaltschaft für den Kuchen zuständig ist.

Anrede!

Ein ganz entscheidender Baustein in der Mauer, die ich als Landesjustizministerin zum Schutz vor der Internetkriminalität hochziehen kann, wird die **Fortbildung** "meiner" Richter und Staatsanwälte sein.

Wir brauchen eine intensive Fortbildung für die Spezialdezernenten und die Ansprechpartner. Und wir müssen allen anderen das Basiswissen vermitteln, das sie brauchen, wenn sie mit der Internetkriminalität befasst sind.

Das heutige Forum soll die Auftaktveranstaltung zu unserer aller Fortbildung sein.

Sie soll unser **Bewusstsein schärfen**. Für die Bedeutung der Internetkriminalität, für die Notwendigkeit ihrer intensiven Bekämpfung und für die Möglichkeiten, die wir dazu schon haben oder aber die wir uns noch schaffen müssen.

Angesichts der Referenten, die wir gewinnen konnten und die ich an dieser Stelle **herzlich willkommen** heiße, bin ich sicher:

Diese Veranstaltung wird halten, was sie verspricht!

Ich freue mich, dass **Herr Präsident Ziercke** vom Bundeskriminalamt heute hier ist, um uns einen Überblick über die Gesamtproblematik zu verschaffen.

Die Strafrechtspraktiker unter uns werden sich vor allen Dingen auf **Herrn Staatsanwalt Dr. Straßer** und **Herrn Kriminalhauptkommissar Hierl** freuen.

Eine besondere Ehre ist es mir, **Herrn Professor Dr. Gercke** unter uns begrüßen zu dürfen. Als Direktor des Cybercrime Research Instituts und Lehrbeauftragter für Medienstrafrecht an der Universität Köln haben Sie sich national wie international einen Ruf erarbeitet, der Ihnen weit voraus eilt. Niemand weiß wohl so gut wie Sie,

sehr geehrter Herr Prof. Gercke,

welche neuen Entwicklungen und aktuellen Herausforderungen auf uns warten -

oder noch warten werden.

Diese Veranstaltung soll aber nicht nur unser Bewusstsein schärfen. Mir geht es vor allem auch darum, dass wir neben dem Internet unser eigenes Netz aufbauen - ein Netz von Kontakten und Informationen.

Der Kampf gegen Cybercrime kann nicht einsam und isoliert geführt werden. Wenn wir gegen das kriminelle Heer der Verbrecher im Netz erfolgreich bestehen wollen, müssen auch wir uns mehr als je zuvor vernetzen und verlinken.

Meine Anregung deshalb:

Nutzen Sie den heutigen Tag! Knüpfen Sie Kontakte und tragen Sie das, was Sie heute hören, auch hinaus zu Ihren Kolleginnen und Kollegen!

Bleiben Sie am Ball - auch in der Zusammenarbeit mit den anderen! Angriffe aus dem World Wide Web können nur selten begrenzt und lokal wirksam abgewehrt werden.

Ich bitte Sie: Seien Sie alle ein link - in unserem Kampf für die Freiheit und Sicherheit der virtuellen Welt!