Strategien gegen Cybercrime

Bei Europol in Den Haag, Niederlande, wird ein Center zur Bekämpfung der Internetkriminalität aufgebaut – das Cybercrime Center EC 3.

In den letzten fünfzehn Jahren hat sich die digitale Welt rasant verändert. Drahtlose Technologien, wie *WiFi* und *WiMAX* ermöglichen den Internetnutzern einen flexibleren Zugang in das Web. Der digitale Handel setzt weltweit acht Billionen Euro um. Fast drei Viertel der Bewohner in der Europäischen Union weisen einen hohen Vernetzungsgrad[1] auf und sind daher für die vielfältigen Modi Operandi im Bereich der Cybercrime ein attraktives Ziel. Der durch diese Kriminalitätsformen angerichtete Schaden wird auf 388 Milliarden Euro geschätzt – das ist einträglicher als der illegale Handel von Marihuana, Kokain und Heroin gemeinsam.[2]

Die Europäische Kommission schlug im April 2012 vor, bei Europol ein Center zur Bekämpfung von Cybercrime einzurichten.[3] Dieser Vorschlag wurde vom Rat in seiner Entschließung vom Juni 2012 unterstützt.[4] Europol hat am 1. Juli 2012 mit der Projektumsetzung begonnen. Geplant, ist dass das Cybercrime Center mit der Bezeichnung EC3 ab dem 1. Jänner 2013 operativ tätig werden soll.

„Die dynamische Entwicklung von elektronischen illegalen Märkten erfordert eine entsprechende und nachdrückliche Prävention und Bekämpfung in einer aktiven Partnerschaft besonders mit dem privaten Sektor, wie

Europol unterstützt die Bekämpfung der schweren Online-Kriminalität unter anderem mit Analytical Workfiles.

Internet Providern, Cyber-Sicherheitsunternehmungen und online – Finanzdiensten", erläuterte Europol-Direktor Rob Wainwright. „Dies kann nur von einer europaweiten zentralen Plattform aus geschehen. Europol verfügt über das nötige Know-how und die Infrastruktur, um diese Aufgabe zu erfüllen." Europol ist bereits mit den *Analytical Workfiles (AWF) TWINS* und *CYBORG* (sämtliche in den Mandatsbereich Europols fallende Formen von Schwer- und organisierter Kriminalität, die online begangen werden) im Kriminalitätsfeld der Bekämpfung der Cybercrime tätig. Ebenso bestehen bei Europol seit einigen Jahren Plattformen zum Erfahrungsaustausch und Vermittlung der „besten Praxis" *(IFOREX)* und der Meldung von Cybercrime *(I-CROS)*.

Aufgaben des Centers sind die Bildung einer Informations- und Analysedrehscheibe über Schwer- und organisierte Kriminalität in diesem Bereich, insbesondere solche mit schwerwiegenden Folgen für die Opfer (z. B. sexueller Kindesmissbrauch im Internet), Meldestelle für Informationen über Cyber-Kriminalität, Unterstützung der Mitgliedstaaten in den Ermittlungen und bei der Einrichtung von eigenen Cybercrime-Kompetenzzentren und Sprachrohr aller mit Ermittlungen gegen Cybercrime befassten Strafverfolgungsbehörden in der Europäischen Union und schließlich die Bekämpfung von Straftaten gegen kritische Infrastruktur und Informationssysteme in der Union.

Angestrebt wird eine umfassende Zusammenarbeit sowohl mit EU-Institutionen, wie der Europäischen Kommission, *CEPOL, Eurojust, ENISA* (Europäische Agentur für Netz- und Informationssicherheit), *EUCTF (European Union Cybercrime Task Force), CIRCAMP (Cospol Internet Related Child Abusive Material Project), CERT-EU (Computer Emergency Response Team) und ECTEG (European Cybercrime Training and Education Group),* als auch mit privaten Organisationen wie beispielsweise der *Microsoft Digital Crimes Unit, World Vision Australia* und *ECPAT (End Child*

ERFOLGREICHE OPERATIONEN

Operation „ICARUS": Europol unterstützte und koordinierte Ermittlungen in 23 Staaten (Österreich, Belgien, Bulgarien, Kroatien, Cypern, Tschechien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Irland, Italien, Luxemburg, Malta, Niederlande, Polen, Rumänien, Schweiz, Slowakei, Spanien, Schweden).

Die Ermittlungen richteten sich gegen ein Pädophilennetzwerk, deren Mitglieder Videos von besonders schweren Formen sexuellen Kindesmissbrauchs, insbesondere von Säuglingen und Kleinkindern, in das Internet gestellt hatten. Die Operation startete Anfang 2011 im Rahmen von CIRCAMP unter der Federführung der dänischen Polizei aufgrund ihrer Erfahrungen in derartigen Ermittlungen. Europol stellte ihr analytisches Know-how zur Verfügung und ermöglichte auch die Zusammenarbeit mit Eurojust und der IKPO Interpol.

Bisher konnten fast 300 Verdächtige ausgeforscht und 113 Personen in allen beteiligten Staaten verhaftet werden. Es wurden auch Pädophilennetzwerke entdeckt, die in verschiedenen Kanälen im Internet operieren, sodass mehr Festnahmen zu erwarten sein werden.

Operation „RESCUE". Die Identifizierung eines weltweiten Netzwerks von mutmaßlichen Pädophilen läuft seit 2009 mit Unterstützung des europäischen Polizeiamtes unter Beteiligung von 13 Staaten (Australien, USA, Belgien, Canada, Deutschland, Griechenland, Island, Italien, Niederlande, Neuseeland, Polen, Rumänien, Spanien, Großbritannien).

Europol erstellte 4.000 Analyseberichte für über 30 Länder. Das bisherige Ergebnis: Fast 800 Verdächtige konnten identifiziert werden, es erfolgten 250 Verhaftungen und 252 Kinder konnten gerettet werden.

FOTO: EUROPOL

Prostitution Child Pornography and Trafficking of Children for Sexual Purposes) – insbesondere in der Prävention und Bekämpfung von sexueller Ausbeutung von Kindern und Kinderpornografie („Outreach"-Programme). Diese Organisationen sind Mitglied der *Virtual Global Taskforce (VGT),* der Europol seit 2011 angehört. Die IKPO Interpol wird als ein weiterer wichtiger Partner der Cybercrime-Plattform angehören und ihre weltweite Infrastruktur und Ressourcen für Ermittlungen im asiatischen Raum einbringen.

Die Errichtung des Cybercrime Centers korrespondiert mit den politischen Strategien wie den Wachstumszielen für Europa 2020[5] , der „Digitalen Agenda für Europa"[6] , dem Stockholm-Programm, sowie dem EU-Politikzyklus 2011 bis 2013 im Strafverfolgungsbereich, wobei die „verstärkte Bekämpfung der Cyberkriminalität und des kriminellen Missbrauchs des Internets durch organisierte Gruppen" eine der acht Prioritäten dieses Zyklus darstellt.[7]

Was bietet Europol? Der umfassende Leistungskatalog besteht aus der Erstellung von Trend- und Risikoanalysen, wobei Europol sich bereits 2010 mit seinem „Threat Assessment Internet Facilitated Organised Crime" *(I-OCTA)* mit den aus der Cybercrime entstehenden Gefährdungen befasst hat. Weiters werden „Early Warning Messages" verfasst und in Zusammenarbeit mit dem privaten Sektor Modelle der Kriminalprävention und strategischer Planung entwickelt *(Public Private Partnership)*.

Die operative Unterstützung durch das EC3 besteht aus der operativen Analyse, forensische Unterstützung durch neue von *Microsoft* entwickelte Technologien wie einer Photo-DNA zur raschen Identifikation insbesondere von Opfern von Kinderpornografie durch Abgleich von Bildern, einer raschen Reaktion auf Cybercrime-Angriffe durch Einrichtung von Notfallteams, Unterstützung von Ermittlungen in Finanz- und Wirtschaftskriminalität, sowie Kinderpornografie im Internet und letztlich dem Schutz von kritischer IT-Infrastruktur in der EU innerhalb des Mandatsbereiches von Europol.

Europol wird in der Erfüllung dieser Aufgaben die Informationsflüsse der Strafverfolgungsbehörden und Institutionen in der EU und auch der privaten

FOTO: EUROPOL

Europol-Zentrale in Den Haag (Niederlande): Das Europol-Center zur Bekämpfung der Internetkriminalität soll mit 1. Jänner 2013 operativ tätig werden.

Einrichtungen verarbeiten und zusammenführen, sowie Aktivitäten der zuständigen Ermittlungsteams im IT-Bereich koordinieren.

Eine weitere wichtige Aufgabe wird der Bereich der Forschung und Entwicklung sein. Hier werden technische Bedrohungsanalysen erstellt und die IT-Systeme auf ihre Verwundbarkeit getestet, Konzepte zur „besten Praxis", Instrumentarien zur Prävention und Bekämpfung von Cybercrime und Ausbildungscurricula entwickelt.

Organisationsstruktur. EC3 wird in der Operativen Abteilung (Operation Department) bei Europol unter dem designierten Leiter Troels Oerting angesiedelt sein. Der Aufbau des Cybercrime Centers hat bereits zu einer raschen Organisationsänderung geführt. Den Kernbereich des Operation Departments bildet der „Information Hub", der Informationsknotenpunkt.

Hier werden Risiko- und Gefahrenanalysen erstellt und hier erfolgt die Koordination von operativen Aktivitäten der Mitgliedstaaten, z. B. im Rahmen von EMPACT und RSO (Regional Support Officer im Bereich der AWF), die Zusammenarbeit mit Drittstaaten und anderen Stellen, wie mit der IKPO Interpol, und die Datenverarbeitung. Umgeben ist der „Information Hub" von den Bereichen Cybercrime Center (EC3), organisierte Kriminalität und Terrorismus. Das Personal wird intern umgeschichtet.

„Europol trägt mit diesem Organisationsmodell den von der Europäischen Kommission auferlegten Einsparungen Rechnung", informierte der Direktor von Europol den Verwaltungsrat in seiner Sitzung im Juni 2012. Denn Europol muss – wie alle europäischen und nationalen öffentlichen Stellen – sparen. So enthält das Budget 2013 eine Reduktion von Finanzmittel in der Höhe von vier Prozent. Darüber hinaus hat die Europäische Kommission für den mehrjährigen Finanzrahmen 2014 bis 2020 eine Personaleinsparung von fünf Prozent vorgesehen.

Gabriele Loidl

[1] EC3 Bulletin, The European Cybercrime Centre Europol, S. 3.
[2] Mitteilung der Europäischen Kommission, Dok. Nr. 8543/12 vom 4.4.2012, ENFOPOL 94, S. 2.
[3] Ebenda
[4] Schlussfolgerungen des Rates, Dok. No. 10604/12, ENFOPOL 154.
[5] Europa 2020 – Eine Strategie für intelligentes, nachhaltiges und integratives Wachstum (KOM(2010) 2020 vom 3. März 2010).
[6] Eine Digitale Agenda für Europa (KOM(2010) 245 endgültig vom 26. August 2010).
[7] EU-Politikzyklus zur Bekämpfung der organisierten und schweren internationalen Kriminalität für den Zeitraum 2011-2013.