

Oberstaatsanwalt Markus Hartmann  
zur Bekämpfung von Cyberkriminalität

# Auf virtueller Streife

Ute Roos



In den letzten Jahren etablierten sich in den Bundesländern bei der Polizei und in der Justiz zentrale Ansprechstellen für Cybercrime, die Unternehmen und Behörden gegen Internetkriminalität beistehen. Oberstaatsanwalt Markus Hartmann berichtet im Interview von seiner Arbeit bei der ZAC NRW.

In Nordrhein-Westfalen entstand 2014 die Zentral- und Ansprechstelle Cybercrime Köln, die 2016 in der neu geschaffenen Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW) aufging. Auch in anderen Bundesländern wurden ähnliche Ansprechstellen in der Justiz und bei der Polizei eingerichtet, an die sich Unternehmen und Behörden bei konkreten Sicherheitsvorfällen wenden können. Sie haben unter anderem Beratungs- und Vermittlungsfunktionen,

beispielsweise in der Zusammenarbeit mit Sicherheitsbehörden (eine Liste der polizeilichen Ansprechstellen ist unter [ix.de/ix1809078](http://ix.de/ix1809078) zu finden).

Die ZAC NRW, die Oberstaatsanwalt Markus Hartmann leitet, ermittelt auch selbst und nimmt innerhalb der Justiz in Nordrhein-Westfalen einige spezielle Funktionen wahr. Sie ist erreichbar unter [zac@sta-koeln.nrw.de](mailto:zac@sta-koeln.nrw.de) oder 0221 477-4922 (24/7-Hotline für Unternehmen und kritische Infrastrukturen).

## ix: Wie sind die Bundesländer bei der Cybercrime-Bekämpfung aufgestellt?

*Hartmann:* Die jeweiligen Organisationsformen der Justiz sind – dem Föderalismus geschuldet – von Bundesland zu Bundesland unterschiedlich. Jedoch gibt es flächendeckend zentrale Organisationseinheiten, die die herausgehobenen, komplexen Cybercrime-Fälle bearbeiten. Für Nordrhein-Westfalen ist die Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen, ZAC NRW, zuständig.

## Worin bestehen die Aufgaben der Zentralstelle?

Wir sind eine operative, bei der Staatsanwaltschaft Köln angesiedelte Hauptabteilung mit sechs Dezernaten. Unsere wichtigste Aufgabe ist die Führung von herausgehobenen Ermittlungsverfahren. Das sind solche, die sich durch verschiedene Kriterien vom Normalfall der Cyberkriminalität unterscheiden, etwa weil die Tatdurchführung technisch besonders komplex ist oder von organisierter Cyberkriminalität verübt wird. Daneben fungieren wir als Ansprechstelle für die Polizei, andere Sicherheitsbehörden und Gerichte in Fragen der Cyberkriminalität. Außerdem ist uns die Aufgabe einer Kontaktstelle für Wissenschaft und Wirtschaft zugewiesen.

Das technisch Mögliche  
mit dem juristisch Erlaubten  
in Einklang bringen

## Wie würden Sie Ihre Arbeit beschreiben?

Zuallererst ist die Arbeit eine juristische. Die Staatsanwältinnen und Staatsanwälte der ZAC NRW verantworten die Führung der Ermittlungsverfahren. Sie beantragen etwa Durchsuchungsbeschlüsse und Haftbefehle bei Gericht und verfassen gegebenenfalls Anklageschriften. Dazu gehört aber immer auch ein erheblicher Anteil technischer Kompetenz, um das, was Strafverfolger technisch können, und das, was sie rechtlich dürfen, in Einklang zu bringen.

## Was ist das Besondere der ZAC NRW?

Die ZAC NRW arbeitet interdisziplinär und vernetzt. Wir versuchen, möglichst umfassende technische Kompetenzen in der Zentralstelle vorzuhalten. So haben wir etwa einen Wirtschaftsreferenten, der als Wirtschaftswissenschaftler auf Finanz-

ermittlungen in Kryptowährungen spezialisiert ist. Gleichzeitig ist uns aber klar, dass wir nie für jedes technische Problem eine Inhouse-Lösung haben werden. Deswegen kooperieren wir sehr eng mit den spezialisierten Polizeidienststellen, etwa des Landeskriminalamtes oder des Bundeskriminalamtes.

Ebenso vertrauen wir aber auf die Kooperationen mit der Wirtschaft. Wenn Sie etwa in einem Unternehmensrechenzentrum sachgerecht Daten sichern wollen, sind Sie stets auf eine vernünftige Zusammenarbeit mit den lokalen Administratoren angewiesen.

#### **Mit welchen Behörden, Unternehmen, Institutionen und so weiter arbeiten Sie beziehungsweise die ZAC NRW zusammen?**

Grundsätzlich sind wir für jede Zusammenarbeit offen, soweit diese mit unserer Rolle als Strafverfolgungsbehörde vereinbar ist. Cybercrime-Bekämpfung kann nur erfolgreich sein, wenn sie als „Shared Mission“ verstanden wird. Je nach Fallkonstellation setzen wir uns mit den erforderlichen Kooperationspartnern zusammen. Das können Universitäten



Quelle: ZAC NRW

## **Markus Hartmann ...**

... ist Oberstaatsanwalt als Hauptabteilungsleiter bei der Staatsanwaltschaft Köln und seit 2016 Leiter der Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen (ZAC NRW). Die ZAC NRW führt Cybercrime-Verfahren von herausgehobener Bedeutung. Sie ist darüber hinaus zentrale Ansprechstelle für grundsätzliche, verfahrensunabhängige Fragestellungen aus dem Bereich der Cyberkriminalität für Staatsanwaltschaften und Polizeibehörden Nordrhein-Westfalens und anderer Länder sowie des Bundes. Ferner steht sie als Kontaktstelle für die Zusammenarbeit mit Wissenschaft und Wirtschaft zur Verfügung, soweit dies mit ihrer Aufgabe als Strafverfolgungsbehörde vereinbar ist.

Auf der diesjährigen von iX, heise Events und eco veranstalteten Sicherheitskonferenz Internet Security Days (Programm und Anmeldung siehe [ix.de/ix1809078](http://ix.de/ix1809078)) wird Oberstaatsanwalt Markus Hartmann die Abschlusskeynote halten.



ebenso sein wie private IT-Sicherheitsfirmen oder andere Behörden, etwa das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Ganz wichtig ist für uns aber auch die Vernetzung mit den Cybercrime-Zentralstellen der Justiz aus anderen Bundesländern. Wenn sich in einem Fall herausstellt, dass die Tatortzuständigkeit eigentlich in Hessen oder Bayern liegt, kann ich ein betroffenes Unternehmen innerhalb weniger Minuten an meine Kollegen der dortigen Zentralstellen weitervermitteln. So ist sichergestellt, dass kein Sachverhalt in Zuständigkeitsfragen untergeht.

#### **Wer tritt eigentlich an Sie oder Ihre Abteilung heran und mit welchen Problemen, Fragen oder Vorfällen?**

Unsere Zuständigkeit für herausgehobene Cybercrime-Fälle bringt es mit sich, dass Anzeigenerstatter häufig größere Unternehmen, Behörden oder Betreiber kritischer Infrastrukturen sind. Wenn der Fall hinreichend komplex ist, führen wir aber auch Ermittlungen wegen Straftaten, die gegen „normale Bürger“ verübt werden.

Viele unserer Ermittlungsverfahren beginnen aber auch durch Initiativ-Ermittlungen der Polizeibehörden. Besonders im Cybercrime-Bereich hat die Poli-

Anzeige

zei in den letzten Jahren massiv an Ressourcen und Kompetenz hinzugewonnen. In den Cybercrime-Dienststellen der großen Polizeibehörden erlebe ich immer wieder technisch ganz herausragende Beamte, die sich mit Experten aus der Wirtschaft ohne Weiteres messen können.

#### Wie ist die Erfolgsquote?

Das letzte veröffentlichte polizeiliche Lagebild für Nordrhein-Westfalen für das Jahr 2017 verzeichnet im Kernbereich der Cyberkriminalität eine Aufklärungsquote von 35,8 %. Eine eigene Statistik der ZAC NRW wird derzeit nicht erhoben.

In unserem Geschäft muss man auch verlieren können

#### Gibt es Grund zum Optimismus und woraus zieht man die Motivation, auf diesem Feld die Kriminellen zu bekämpfen?

Bei der Aufklärungsquote ist sicherlich noch Luft nach oben. In unserem Geschäft muss man auch verlieren können. Das bringt die technische Komplexität der Fälle manchmal leider mit sich. Mir ist allerdings kaum ein Fall erinnerlich, in dem wir nicht zumindest den Tathergang haben klären können. Auch das halte ich für einen Erfolg, denn mit den Erkenntnissen zur Angriffsweise kann man andere potenzielle Opfer vorwarnen.

#### Ihre größten Erfolge und Misserfolge?

Für einen Staatsanwalt ist es immer schwer, über seine Fälle detailliert zu sprechen, denn die Anzeigenerstatter und Geschädigten müssen sich auf den vertraulichen Umgang mit ihren Belangen verlassen können. Würde ich zum Beispiel einzelne Ermittlungserfolge bei unternehmensbezogener Cyberkriminalität öffentlich ausführlich kommentieren, würde dies die Anzeigebereitschaft zukünftiger Betroffener sicher negativ beeinflussen.

Wir haben uns in unserer Arbeit einige Schwerpunkte gesetzt. Einer davon ist die Bekämpfung der Darknet-Kriminalität, denn der Handel mit Drogen und Waffen verlagert sich immer mehr ins Netz. Ich freue mich sehr, dass wir in zahlreichen Verfahren Darknet-Drogendealer und -Waffenschieber haben erfolgreich anklagen können.

Wir engagieren uns aber auch in Querschnittsthemen. Eines der Dezernate der ZAC NRW befasst sich etwa mit der Be-

kämpfung der Hasskriminalität im Netz. Unser Motto ist hier „Verfolgen statt nur Löschen“. Dazu arbeiten wir mit der Landesanstalt für Medien NRW, dem Landeskriminalamt NRW und verschiedenen Medienunternehmen zusammen.

#### Wie schätzen Sie die weiteren Entwicklungen auf dem Gebiet Cybercrime ein?

Es wird nicht weniger. Und leider auch nicht einfacher. Wir sehen zunehmend zielgerichtete, hochkomplexe Kompromittierungen und Angriffe aus dem Graubereich zwischen organisierter und drittstaatlich induzierter Cyberkriminalität. Für die Strafverfolger ist es eine Herausforderung, ihre Handlungsfähigkeit in diesem Umfeld zu bewahren. Umso mehr freut es mich, dass die ZAC NRW zum Jahresanfang 2018 erheblich verstärkt worden ist. Bald werden wir mit 21 spezialisierten Staatsanwältinnen und Staatsanwälten Cyberkriminalität verfolgen.

#### Sind Sie besorgt um die deutsche Wirtschaft und die kritischen Infrastrukturen hierzulande?

Bei dieser Frage muss ich zurückhaltend antworten, da ich naturgemäß immer nur die Fälle sehe, in denen etwas schiefgegangen ist. Die Qualität der Angriffe ist in der letzten Zeit jedoch deutlich gestiegen, sodass eine gesunde Sorge berechtigt ist.

Cybersicherheit ist eine Dauerbaustelle

#### Wie schätzen Sie die IT-Sicherheit und Wehrhaftigkeit der deutschen Wirtschaft und der Betreiber kritischer Infrastrukturen ein?

Im Unterschied zu der Situation vor einigen Jahren haben wir meiner Wahrnehmung nach kein Awareness-Problem mehr. Die Unternehmen wissen, dass sie einer ständigen Bedrohung durch Cyberkriminelle ausgesetzt sind. Leider handeln nicht alle nach dieser Erkenntnis, weil Cybersicherheit immer auch Geld und Mühe kostet.

Ich wünsche mir aus den Erfahrungen unserer Ermittlungsverfahren, dass die Unternehmen mehr in qualifizierte Sicherheitsmaßnahmen investieren und verstehen, dass Cybersicherheit nicht schon mit dem Kauf von Produkt X oder der Anschaffung von Appliance Y gewährleistet ist. Cybersicherheit ist eine Dauerbaustelle.

#### Gibt es Aufklärungs- und Handlungsbedarf in der Bevölkerung und der Wirtschaft?

Eindeutig ja! Cyberkriminalität entwickelt sich dynamisch. Was heute noch ein Angriffsszenario ist, wird morgen durch etwas ganz anderes abgelöst. Hier muss die Wirtschaft Schritt halten. Mit Blick auf die Bevölkerung sehe ich aber auch die Hersteller von Hard- und Software in der Pflicht, bessere, das heißt sicherere Produkte anzubieten. Ich glaube nicht, dass wir von „Otto Normaluser“ verlangen können, sich detailliert mit Schwächen im Design von Prozessoren auseinanderzusetzen.

#### Ist das rechtliche Instrumentarium ausreichend für eine Verfolgung von Cyberkriminellen?

Auf die Frage gibt es keine einfachen Antworten. Es ist ausgesprochen komplex, einen vernünftigen und sachgerechten Ausgleich zwischen den Erfordernissen wirkungsvoller Strafverfolgung und grundrechtlichen Positionen im Internet herzustellen. Klar ist: Das Internet ist kein rechtsfreier Raum. Wo sich Ansätze zeigen, dass Strafverfolgung nicht mehr durchdringt, muss der Gesetzgeber nachjustieren. Die Vorschriften, nach denen wir heute E-Mails beschlagnahmen, standen fast wortgleich bereits in der ersten Fassung der Strafprozessordnung von 1877. Es ist aus meiner Sicht daher nicht fernliegend, besonders das strafprozessuale Instrumentarium an die Wirklichkeit des digitalen Zeitalters anzupassen.

#### Wie gestaltet sich die (oft unerlässliche) Zusammenarbeit mit anderen Ländern? Gibt es hier Hindernisse?

Die Verbesserung der Zusammenarbeit bei der Rechtshilfe ist aus meinem Erleben eine der Erfolgsgeschichten der jüngeren Zeit. Die ZAC NRW arbeitet mit vielen Ermittlungsbehörden ausländischer Staaten vertrauensvoll zusammen. Wenn es die Sache erfordert, können wir auf Basis dieser Zusammenarbeit binnen weniger Stunden Maßnahmen durchführen.

Gerade bei der Frage des transnationalen Datenzugriffs ist durch den US-amerikanischen CLOUD Act und die jüngeren Vorschläge der EU-Kommission erhebliche Bewegung in die rechtspolitische Diskussion gekommen. Ich bin hoffnungsvoll, dass die Möglichkeiten der internationalen Zusammenarbeit kurzfristig weiter verbessert werden können. (ur@ix.de)