Innovationspreis HFP Reto Habermacher →

Verdeckte polizeiliche Einsätze bei Cybercrime

Für seine Diplomarbeit «Proaktive Massnahmen zur Bekämpfung der digitalen Kriminalität bei der Kantonspolizei St. Gallen» erhielt Damian Broger vor kurzem den Innovationspreis HFP Reto Habermacher verliehen. Im Interview mit *police* erläutert der Preisträger, weshalb die traditionelle Repression bei der digitalen Kriminalität nur einen geringen Effekt erzielt und welche Massnahmen Erfolg versprechender sind.

Interview: Markus Nobs; Fotos: SPI

Interview

Herzliche Gratulation zur ehrenvollen Auszeichnung! Was bedeutet dir der Gewinn dieses Preises?
Herzlichen Dank für die Glückwünsche. Der Gewinn des Innovationspreises HFP Reto Habermacher freut mich sehr und hat gleich mehrere Bedeutungen für mich. Einerseits ist dies eine grosse Anerkennung für all die Aufwände, welche bei mir, meinem Team sowie allen Beteiligten – insbesondere Auftraggeber, Mentor, Interviewpartner, Teilnehmende an Umfrage und Workshop – während dem Erstellen der Diplomarbeit entstanden waren. Nicht vergessen darf man dabei auch die vielen Entbehrungen meiner Familie, zumal ich den grössten Teil der Diplomarbeit in meiner Freizeit geschrieben hatte.

Andererseits bedeutet der Preis für mich und vermutlich alle, welche sich im Bereich der Bekämpfung der digitalen Kriminalität engagieren, dass wir mit unseren innovativen und oftmals neuen Methoden und Ansätzen auf dem richtigen Weg sind. Im relativ neuen Tätigkeitsbereich «Bekämpfung der digitalen Kriminalität» stossen herkömmliche Ermittlungsansätze schnell an ihre Grenzen. Hier sind kreative Ansätze und ein interkantonaler, im Idealfall sogar internationaler, offener Austausch gefragt.

Weshalb erzielt Repression im Zusammenhang mit der digitalen Kriminalität bei international agierenden Täterschaften nur einen sehr geringen Effekt?
Im Gegensatz zur klassischen «analogen» Kriminalität erfordern Tatausführungen im digitalen Raum kein Handeln am Erfolgsort. Somit können digitale Delikte aus jedem Land der Welt verübt werden. Zusätzlich können die Täter eine Vielzahl von weltweit vorhandenen Online-Dienstleistungen nutzen, welche Ihnen bei der Verschleierung der Spuren helfen. Diese internationale Dimension bei den Ermittlungen erfordert, zwecks Identifizierung und Zuführung der Täterschaft zur Strafverfolgung, effiziente Amts- und Rechtshilfeverfahren mit den jeweiligen Ländern. Und zwar am Aufenthaltsort der Täterschaft wie am Standort der genutzten Dienstleistungen. In der Realität stellen wir aber fest, dass einige der angefragten Länder entweder nicht mit uns kooperieren oder im Falle einer Zusammenarbeit die Verfahren sehr ineffizient, formell und langwierig sind. In Bezug auf den repressiven Effekt bei der Täterschaft werden als Konsequenz der aktuellen Situation nachfolgende Werte ersichtlich:

Bei knapp 90 % aller Fälle handelt die Täterschaft aus dem Ausland.

Bei knapp 90 % aller Fälle handelt die Täterschaft bei digitaler Kriminalität aus dem Ausland. Jedoch kann nur in vier von zehn Fällen die Täterschaft einem konkreten Land zugeordnet werden. In jedem 40. Fall kann die Täterschaft mittels internationaler Amts- oder Rechtshilfe identifiziert werden. Schlussendlich gelingt es jedoch nur in knapp 0,5 % aller Fälle, die ausländische Täterschaft der Strafverfolgung zuzuführen.

Bei diesen Werten handelt es sich mangels statistischer Angaben um Mittelwerte der geschätzten Angaben von 25 Fachspezialisten des NEDIK [Anm. d. Red.: Netzwerk digitale Ermittlungsunterstützung Internetkriminalität], welche im Rahmen der HFP mittels Online-Umfrage erhoben wurden.

Preisübergabe an Damian Broger durch den Direktor des SPI, Stefan Aegerter (links) sowie Emmanuel Fivaz, Vizepräsident VSPB (rechts im Bild).

Aus diesen Zahlen schliesse ich, dass in diesem Deliktsbereich die internationale Zusammenarbeit nicht zufriedenstellend funktioniert und die Fokussierung rein auf Repression nicht den gewünschten Effekt erzielt.

Welche proaktiven Massnahmen sind demzufolge Erfolg versprechender bei der Bekämpfung der digitalen Kriminalität?
Grundsätzlich alle Massnahmen, welche eine frühzeitige Störung der Täterschaft bei der Tatvorbereitung und/oder Tatausführung erzielen oder gar die Tatinitialisierung hemmen. Zur frühzeitigen Störung der Täterschaft zähle ich hier mögliche Massnahmen zur Unterbrechung der Kommunikation zwischen Täter und Opfer, z. B. Missbrauchsmeldungen an Hoster, Domain-Sperrungen, Melden von Fake-Profilen zwecks Überprüfung oder Löschung sowie des Geldflusses, insbesondere Meldung täterischer Kontoinformationen an Finanzintermediäre. Ein anderer Ansatz ist ein Angriff auf die Reputation respektive das Vertrauen in die Täterschaft, z. B. absichtlich schlechte Bewertungen auf Darknet-Marktplätzen für täterische Angebote. Idealerweise erzielen die gewählten Massnahmen bei der Täterschaft gleich in mehreren Bereichen einen Effekt. So beispielsweise bei der Zusammenarbeit mit einem schweizerischen Startup, wo Behörden, aber auch Private täterische Adressierungselemente melden können und diese nach erfolgter Prüfung in einer internen Watchlist eingetragen werden. Diese Watchlist wiederum können alle angeschlossenen Partner, zum Beispiel Finanzintermediäre und andere Internet-Dienstleister, zeitverzugslos in ihren internen Compliance-Systemen integrieren.

Eine deiner vorgeschlagenen Massnahmen ist, dass sich die Polizei selbst als «Money Mule» ausgeben sollte. Worum handelt es sich hier und was ist der Nutzen?
Bei den Cybercrime-Wirtschaftskriminalitäts-Phänomenen hat die Täterschaft das Motiv, eine Vermögensverschiebung von den Geschädigten zur Täterschaft zu erzielen. Der konstante Anstieg der Fallzahlen sowie die immer höher werdenden Deliktsummen führten dazu, dass seitens Banken Massnahmen zur Betrugsprävention eingeführt wurden. Auch seitens Bevölkerung wird infolge Präventionskampagnen eine Zahlung auf ein ausländisches Konto kritisch gesehen. Die Täterschaft reagierte auf diese Massnahmen, indem sie beim Finanzfluss inländische Zwischenstellen, sogenannte Money Mules, als Relais einbauten. Durch den Einsatz der Money Mules wird den Geschädigten eine inländische Zahlung suggeriert und gleichzeitig für die Ermittelnden die Analyse des Geldflusses erschwert.

Als proaktive Lösung für dieses Problem empfehle ich einen verdeckten polizeilichen Einsatz auf Basis des kantonalen Polizeigesetzes. Indem die Polizei auf diverse täterische Anzeigen zur Rekrutierung von Money Mules reagiert, sich anwerben lässt und deliktische Zahlungen auf verdeckte polizeiliche Konten zulässt, erzielt sie gleichzeitig zwei gewünschte Effekte: Einerseits kann der Zahlungsfluss von deliktischen Geldern unterbrochen und diese Gelder den Geschädigten zurücktransferiert werden, andererseits kann bei den Money-Mule-Rekrutierenden die Reputation respektive bei deren Kunden das Vertrauen in diese vermindert werden. Daher ist es auch kein Problem, sondern sogar wünschenswert, wenn die Täterschaft am Ende von verdeckten Einsätzen der Polizei als Money Mule erfährt. So kann sie sich beim Rekrutieren von neuen Money Mules nicht mehr sicher sein, ob es sich um die Polizei oder wirklich um eine ahnungslose Privatperson handelt.

In deiner Arbeit wird auch die proaktive Massnahme beschrieben, dass die Polizei – inkognito selbstverständlich – absichtlich schlechte Bewertungen für täterische Ange-

bote vergeben sollte. Wie muss man sich das vorstellen, wie auf Ricardo?
Im Grundsatz nutzt diese proaktive Massnahme die Bewertungsmöglichkeiten des Verkäufers. So wie wir es beispielsweise mit den Sternen und dazugehörenden Bemerkungen auf Ricardo oder Amazon kennen. Der Einsatz dieser Massnahme macht aber insbesondere auf Marktplätzen Sinn, wo seitens der Marktplatzbetreiber keine Kooperation mit der Polizei besteht, z. B. im Darknet oder auf Telegram-Channels. In diesen Fällen ist es meistens nicht möglich, das Angebot direkt löschen zu lassen.

Unsere Erfahrungen zeigen jedoch, dass sich insbesondere im Bereich des Hightech Crime die Täterschaft oftmals arbeitsteilig organisiert. Es existiert ein weitverzweigtes Netz von Partnern und Playern, jeder mit seinen eigenen Spezialisten und klar definierten Aufgabenbereichen. Die jeweiligen Leistungen werden vor allem im Darknet in Foren oder auf Marktplätzen angeboten. Auch auf diesen Plattformen existiert für Käufer wie auch Verkäufer oftmals ein Bewertungssystem. Dies eröffnet der Polizei die proaktive Möglichkeit, dass sie mittels absichtlich schlechten Bewertungen für illegale Angebote einen nachhaltigen Angriff auf die Reputation der Verkäufer vornehmen kann.

Aus deiner Arbeit geht hervor, dass die Staatsanwaltschaft manchmal der Forderung der Polizei nach einer raschen Sperrung von betroffenen Konti nicht nachkommt, sondern diese lediglich ediert [Anm. d. Red.: Ersuchen um Auskunft der wirtschaftlich Berechtigten]. Spielt dies nicht einer Täterschaft in die Karten?
Ja, leider ist das genauso. Unsere Erfahrungen zeigen, dass ein Money-Mule-Konto durch die Täterschaft innert kurzer Zeit mehrfach zur Geldwäsche genutzt wird. Daher ist es äusserst wichtig, diese Money-Mule-Konten baldmöglichst zu sperren und dabei im Idealfall auch noch deliktische Gelder, welche sich auf dem Weg zwischen Geschädigtem und Täterschaft befinden, sicherzustellen. Leider erfolgen seitens Staatsanwaltschaft oftmals lediglich Editionen der betreffenden Konten, was dazu führt, dass diese für die Geldwäsche immer noch genutzt werden können. Diesbezüglich sind mir deutlich zu viele Fälle bekannt, in welchen die gleichen Money-Mule-Konti über einen längeren Zeitraum durch mehrere kantonale Staatsanwaltschaften ediert, aber nicht gesperrt wurden. ←

Die Antworten zu den Interviewfragen repräsentieren die Meinung des Interviewten und widerspiegeln unter Umständen nicht die Meinung des VSPB.

Marianischer Saal in Luzern: Würdiger Durchführungsort der Preisverleihung.