Auszug aus der Personalzeitung des kantonalen Personals vom April 2017

Betrügern auf der Spur

Die neuen Medien und das Internet bieten in der heutigen Zeit fast unendliche Möglichkeiten. So positiv dies ist, in den Tiefen der virtuellen Welt lauern auch allerhand Gefahren. Als Cyberermittler bei der Zuger Polizei heftet sich **Andreas Eugster** seit Sommer 2016 an die Fersen der Internetbetrüger.

Andreas Eugster, wie sind Sie zu Ihrem heutigen Aufgabenbereich gekommen?
Nach meiner Berufsausbildung bei der Swisscom Schweiz AG absolvierte ich an der Zürcher Hochschule für Angewandte Wissenschaften ein Informatikstudium. Da mich das Thema Internetsicherheit wie auch die juristischen Fächer besonders stark interessierten, wurde mir sehr schnell klar, dass ich nach dem Studium im Bereich der Strafverfolgung tätig sein möchte. Aus diesem Grund absolvierte ich anschliessend die Polizeischule. Während meinem Dienst bei der Regionalpolizei bei der Kantonspolizei Zürich schloss ich an der Hochschule Luzern einen Weiterbildungsmaster im Bereich Wirtschaftskriminalistik und IT Forensik ab. Seit Juli 2016 bin ich nun als Cyberermittler bei der Zuger Polizei tätig.

Wann kommen Sie zum Einsatz?
Meine Fachkompetenz ist immer dann gefragt, wenn es um Cyberkriminalität und Betrugsdelikte mit Informatikhintergrund geht. Dies ist in der heutigen Zeit mit allen Möglichkeiten, die das Internet und die neuen Medien bieten, fast täglich der Fall. Die Arbeit nimmt stetig zu und es stellen sich mir immer neue Herausforderungen, was meine Tätigkeit sehr spannend macht.

Was muss man sich unter einem Cyberermittler vorstellen?
Ich löse verschiedene IT-Straffälle von A bis Z, dies bedeutet, von der Strafanzeige über die Ermittlung bis zur Verhaftung von möglichen Tätern. Dazu gehört auch die Befragung der beschuldigten Personen wie auch der Opfer. Zudem berate ich meine Kolleginnen und Kollegen der Zuger Polizei bei Fällen in IT-ermittlungstechnischen Belangen. Ein ganz wichtiger Punkt sind auch die präventiven Ermittlungen im Internet. Dies alles erfordert ein Kombi-Fachwissen aus den Bereichen Strafrecht, Informatik und polizeitaktischen Fähigkeiten. Als Cyberermittler muss man wissen, wie man sich in einem virtuellen Umfeld rechtlich korrekt und gleichzeitig auch unerkannt bewegen kann.

Wie sieht bei Ihnen ein «normaler» Tagesablauf aus?
Neben Sitzungen, Beurteilungen von Lagebildern, Strategieentwicklungen und Hausdurchsuchungen stehen natürlich die Ermittlungen im Netz im Fokus meiner Tätigkeit. Da kann es schon mal vorkommen, dass ich mich stundenlang im Internet bewege, sei es um in einem Online-Portal eine Straftat nachzuvollziehen, um gefälschte Pseudonyme oder E-Mailadresse «zu verfolgen», die wahre Identität einer Person herauszufinden oder einen Anfangsverdacht einer Straftat mit weiteren öffentlichen Informationen aus dem Internet zu verdichten. Fast immer ist auch eine Zusammenarbeit mit externen Stellen gefragt, denn Cyberdelikte kennen keine Landes- und schon gar keine Kantonsgrenzen.

Wie wichtig ist Ihre Tätigkeit?
Da es in der heutigen Zeit kaum mehr Straftaten gibt, die nicht irgendwelche elektronischen Spuren hinterlassen, darf man die Cyberermittlung nicht vernachlässigen. Allerdings ist meine Arbeit als Cyberermittler nur eines von ganz vielen Puzzleteilen der Polizeiarbeit und einer erfolgreichen Strafverfolgung. So werden die sichergestellten Daten zum Beispiel durch die Kollegen der IT-Forensik fachgerecht gesichert und für die weiteren Ermittlungen gerichtsverwertbar aufbereitet. Meine Kolleginnen und Kollegen der anderen Fachbereiche ermitteln auf ihrem Gebiet, während ich die Cyberkomponente bearbeite. Unser gemeinsames Ziel ist es, Cyberkriminelle sowie auch andere Täter zu überführen und zur Rechenschaft zu ziehen.

Mit was für Straftaten haben Sie zu tun?
Die Bandbreite ist enorm und die Fantasie der Cyberkriminellen kennt beinahe keine Grenzen. Die Vorfälle erscheinen wellenartig und haben meistens nur ein Ziel; nämlich die Bereicherung der Täter. Ein bekanntes Phänomen ist das sogenannte «Phishing». Dabei versuchen die Täter, an Passwörter zu gelangen, um Zugang zu vertraulichen Daten ahnungsloser Internetbenutzer zu erhalten. Dies können beispielsweise Kontoinformationen für das E-Banking sein. Ein weiteres Phänomen, das meistens jüngere Menschen betrifft, ist das «Sexting». Damit gemeint ist der Austausch intimer Fotos oder Videos per Computer oder Smartphone. Viele Personen sind sich der möglichen Konsequenzen wie einer späteren Erpressung nicht bewusst. In der jüngsten Vergangenheit hatten wir aber auch mehrere Fälle von sogenannten «Money Mules». Bei dieser Betrugsform offerieren die Täter interessierten Personen eine Teilzeitstelle mit guten Verdienstmöglichkeiten; in Tat und Wahrheit werden die Privatpersonen aber für illegale Geldüberweisungen missbraucht. Diese und noch viele weitere Fälle beschäftigen mich und meine Kolleginnen und Kollegen täglich.

Wie gehen die Täter genau vor?
Die Tricks von Cyberkriminellen und Internetbetrügern werden immer perfider und sie nutzen die scheinbare Anonymität im Netz schamlos aus. Sie gehen auch äusserst professionell vor und haben grosses psychologisches Geschick. So gelingt es ihnen immer wieder, das Vertrauen ihrer Opfer zu gewinnen, diese zu beeinflussen und zu Geldüberweisungen zu veranlassen.

Wie kann man sich gegen solche Betrüger schützen?
Ganz allgemein kann man sicher sagen, dass man nie persönliche Daten an unbekannte Personen weitergeben soll – schon gar keine Bank- und Kontoinformationen. Auch raten wir dringend davor ab, E-Mails von unbekannten Personen zu öffnen und nie auf darin enthaltene Links oder Anhänge zu klicken. Auch unerwartete E-Mails von vermeintlich bekannten Absendern bergen Gefahren, sollten kritisch geprüft und im Zweifelsfall ungelesen gelöscht werden.

Sind Sie als Spezialist also rundum sicher?
Gegenfrage, gibt es denn eine hundertprozentige Sicherheit? So wie wir als Polizisten Opfer eines Einbruchs oder Trickdiebstahls sein können, ist es sicher auch möglich, dass ich einem Internetbetrüger auf den Leim gehe, was auch schon fast passiert wäre. Auch ich bewege mich im Internet und kaufe mit meiner Kreditkarte ein. Ich versuche jedoch, genau zu überprüfen, ob alles seriös ist und keine Personen mit krimineller Energie dahinter stecken. Wir alle sollten uns im Klaren sein, dass nicht alles, was im Internet vertrauenswürdig aussieht, auch wirklich vertrauenswürdig ist.

Frank Kleiner