Betrugsbekämpfung im Internet

Das Team Internet und Cybercrime der Zollfahndung bekämpft Zoll- und Abgabenbetrug im Internet. Dazu zählen die Beweissicherstellung, die Wiederherstellung gelöschter Daten sowie die Täteridentifikation.

Vom Zigarettenschmuggel im großen Stil mit einem Schaden von 50 Millionen Euro über die Ermittlungen in der Steueraffäre rund um einen bekannten Fußballklub 2004 bis hin zu geschmuggelten Dörrpflaumen – das zeigt die Vielfalt und Bandbreite des Einsatzfeldes des im Bundesministerium für Finanzen im Bereich Betrugsbekämpfung eingegliederten Zollfahndungsteams Internet und Cybercrime.

Vor kurzer Zeit deckten die Cybercrime-Spezialisten in Zusammenarbeit mit Finanzpolizei und dem EKO Cobra/DSE einen Sozialbetrugsfall in Kärnten auf, bei dem ein Security-Unternehmen seine 537 geringfügig beschäftigten Mitarbeiter weit mehr als offiziell dokumentiert arbeiten ließ und schwarz bezahlt hat. Fast 500 von ihnen bezogen darüber hinaus illegalerweise Arbeitslosengeld.

„Unsere Cybercrime-Spezialisten haben sämtliche Computerdaten dazu gesichert und ausgewertet“, berichtet Dr. Herwig Heller, Leiter der Abteilung für Betrugsbekämpfung Steuer und Zoll des Bundesministeriums für Finanzen. Auch Auswirkungen der Corona-Pandemie erkennen die Ermittler im Bereich des versuchten Förderungsmissbrauchs im Rahmen der Corona-Hilfen. „Natürlich ist oberstes Gebot, allen jenen zu helfen, die Hilfe brauchen – diejenigen, die sich in der Krise bereichern wollen, haben hingegen mit null Toleranz zu rechnen“, sagt Abteilungsleiter Heller. Die Umsetzung der Förder- und

Herwig Heller: „Am verletzlichsten ist der Verbraucher – auch im Internet.“

Hilfsmaßnahmen wird daher seit Beginn der Krise schwerpunktmäßig kontrolliert.

Internetbetrug. Die Zollfahnder des Teams Internet und Cybercrime beschäftigen sich mit der Bekämpfung des Zoll- und Abgabenbetrugs im Internet in all seinen Facetten. „Die großen Arbeitsbereiche lassen sich in Forensik, Internetermittlung und technische Observation untergliedern“, erklärt der Abteilungsleiter. „Dazu zählen typischerweise die Sicherstellung von Beweisen und die Wiederherstellung von gelöschten Daten auf Computern. Aber auch die Marktbeobachtung hinsichtlich aktueller Trends des elektronischen Geschäftsverkehrs insbesondere des Versandhandels, der operativen Internetermittlung und nicht zuletzt die Täteridentifikation sind Aufgaben unserer Spezialisten.“ Auch wenn aufgrund der unterschiedlichen Fälle kein Tag dem anderen gleicht, sind die Grundzüge der Tätigkeiten ähnlich: „Die Arbeit umfasst hauptsächlich klassische Analysetätigkeiten, die einerseits am Computer, aber auch an den Analysestationen im Forensiklabor stattfinden“, erklärt Heller. „Nach erfolgter Analyse wird der Sachbearbeiter einbezogen, der mit dem jeweiligen Fall betraut ist. Danach wird eine gemeinsame Ergebniskontrolle durchgeführt. Die Analyse wird dementsprechend verfeinert. Dieser Ablauf wiederholt sich, bis Beweismittel gefunden werden. Das Team wird auch zu Hausdurchsuchungen beigezogen. Der Bereich Internet und Cybercrime entwickelt sich besonders dynamisch. Schulungen und Vortragstätigkeiten zu den Themen Cybercrime, Internetrecherche und virtuelle Währungen sind fester Bestandteil im Arbeitsalltag der Spezialisten.“

Digitalisierung als Gründungsanstoß. Gegründet wurde die Einheit 2001, damals als zusätzliches Arbeitsfeld der Zollfahndung. Der fortschreitende Zugang Privater zum Internet und die steigende Digitalisierung machten vor allem anhand vermehrter privater Warenbestellungen aus Drittländern deutlich, dass man hier Möglichkeiten zur Kontrolle braucht. Im Mai 2004 entstand dann eine eigenständige Einheit. Das

BEGRIFFSLEXIKON

Cloud-System: IT-Infrastrukturen wie Speicherplatz, Rechenleistung oder Anwendungssoftware werden über ein Rechnernetz zur Verfügung gestellt, ohne dass diese auf dem lokalen Rechner installiert sein müssen.

Cybercrime: im „engeren Sinne“ umfasst der Begriff jene Straftaten, bei denen Angriffe auf Daten oder Computersysteme unter Ausnutzung der Informations- und Kommunikationstechnik (IKT) begangen werden – z. B. Datenbeschädigung, Hacking, DDoS-Attacken. Unter Cybercrime „im weiteren Sinne“ versteht man Straftaten, bei denen die IKT zur Planung, Vorbereitung und Ausführung für herkömmliche Kriminaldelikte eingesetzt wird, wie z. B. Betrugsdelikte, Kinderpornografie. Diese Straftaten können praktisch jede Form von Kriminalität annehmen.

Forensik: ist ein Sammelbegriff für wissenschaftliche und technische Arbeitsgebiete, in denen kriminelle Handlungen systematisch untersucht werden.

Kryptowährungen: bezeichnen digitale Zahlungsmittel, die auf verschlüsselten digitalen Signaturen basieren.

Thin Client: bezeichnet meist einen Computer, der über ein Netzwerk mit einem Server verbunden ist und dessen Ressourcen nutzt. Stellt die Schnittstelle zur Kommunikation mit einem Server dar.

FOTO: BMF/CITRONENROT

IT-Ermittler der Zollfahndung beschäftigen sich mit der Bekämpfung des Zoll- und Abgabenbetrugs im Internet.

Foto: BMF/Citronenrot

Team ist bundesweit zuständig und damit auch in ganz Österreich im Einsatz. Es steht Einheiten des Zolls und der Finanzverwaltung, insbesondere den IT-Teams der Steuerfahndung, mit seiner Expertise und Einsatz zur Verfügung und wird zu vielen Fällen und Ermittlungen beigezogen. Eine genaue Fallzahl lässt sich nicht festmachen, da es sich um gemeinsame Erfolge handelt.

Die genaue Anzahl der Fahnder in diesem Spezialbereich wollte man aus ermittlungstaktischen Gründen nicht offenlegen. Jedenfalls bedarf es neben den allgemeinen Anforderungen an Zollfahnder in diesem speziellen Bereich hoher technischer Anforderungen. „Technisches Verständnis ist Voraussetzung für das Team, weshalb bei Anwärtern Vorbildung gern gesehen ist, beispielsweise einer technischen Schule“, sagt Heller. „Schulungen externer Anbieter, im Besonderen sind dies oft Schulungen von Forensiksoftware-Herstellern, runden die Aus- und Weiterbildung ab. Nicht zuletzt ist es unerlässlich, dass sich die Mitarbeiter in diesem Bereich auch autodidaktisch weiterbilden.“

Die Hauptdelikte, mit denen sich diese Spezialeinheit des Zolls auseinandersetzt, reichen von Datenangriffen im Internet aller Art bis hin zu kriminellen Handlungen, die sich diese Technologien zu Nutze machen. Da somit Schutz- und Sicherungsfunktionen wahrgenommen werden, tragen die Cybercrime-Spezialisten auch Waffen. „Mittlerweile allgemein bekannte Cybercrime-Delikte sind Phishing, also Versuche, durch gefälschte Websites an persönliche Nutzerdaten zu kommen, oder auch die Infizierung des Computers durch unbemerkte Installation von Schadsoftware auf dem Rechner“, erklärt Heller. „Auch da gibt es immer wieder Versuche, diese Methoden im Bereich des BMF auf Kosten der Steuerzahler anzuwenden. Datenschutz ist nicht umsonst ein viel diskutiertes Thema. Am verletzlichsten ist der Verbraucher – auch im Internet. Kriminelle nutzen Kryptowährungen vor allem für Betrug und Erpressung, aber auch zur Geldwäsche.“ Enge Kontakte gibt es mit dem Bundeskriminalamt, insbesondere dem *Cybercrime-Competence-Center (C4),* hinsichtlich virtueller Währungen. Auch im Bereich der Wirtschaftskriminalität gibt es immer wieder Fälle, bei denen gemeinsam ermittelt wird.

„Die globale Dimension und die unterschiedlichen Rechtslagen in betreffenden Ländern stellen eine Herausforderung dar“, sagt Heller. „Beispielsweise aus dem amerikanischen Raum sind nur schwer Auskünfte zu erhalten. Oft werden diese verweigert oder auf eine richterliche Anordnung gepocht. Viele Verfahren sind bei uns allerdings verwaltungsbehördlich geführt, weshalb es solche Anordnungen nur eingeschränkt gibt. Eine weitere Herausforderung ist die Sicherung von Daten in Cloudsystemen, die immer populärer werden“ – und damit auch ein großes Zukunftsthema im Bereich Cybercrime darstellen. Beweismittel sind global verstreut, ohne Beschränkung durch nationale Grenzen, oftmals auch in Staaten ohne Amts- und Rechtshilfe.

Die klassische Festplattensicherung hat ausgedient, Computer sind als „Thin Clients“ über ein Netzwerk mit einem Server verbunden und bedienen sich dessen Ressourcen. Auch die Verschlüsselung als Standard in Betriebssystemen wird ein gewisser Erschwernisfaktor hinsichtlich der Entschlüsselung bleiben. Und die virtuelle Welt entwickelt sich weiter: Beweismittel, die sich in virtuellen Maschinen verstecken, verschlüsselte virtuelle Maschinen und virtuelle Maschinen in der Cloud – die Bekämpfung von Cybercrime bleibt auch in Zukunft eine Herausforderung.“

Julia Brunhofer/Herbert Zwickl