Miami (Florida): Gemeinsames Einschreiten von Europol, FBI, USPIS, der lokalen Polizeibehörden in Miami, SWAT-Polizisten und österreichischen Ermittlern gegen den von „Soko-Mozart"-Mitgliedern ausgeforschten Haupttäter.

Betrügerische Überweisungen

Ermittlungsteams sechs europäischer Länder forschten eine Gruppe von Cyber-Kriminellen aus, die weltweit E-Banking-Nutzer abzockten. Die „Soko Mozart" spielte bei den Ermittlungen eine führende Rolle.

Der Salzburger Polizist Michael Manger ermittelte 2011 in einem Fall von betrügerischer Geldüberweisung über das Internet. Ein Mann hatte Anzeige erstattet, dass ohne sein Wissen Geld von seinem Konto auf ein anderes Konto überwiesen worden war. Der Empfänger des Geldes war als „Finanzagent" tätig. Er kassierte eine Provision dafür, dass er sein Konto zur Verfügung stellte und weitere Dienste leistete. Außer dem Salzburger wurden zahlreiche weitere Netbanking-Nutzer österreichischer Banken durch betrügerische Überweisungen geschädigt. Manger kam bei seinen Ermittlungen einer kriminellen Struktur auf die Spur, die Betrügereien dieser Art in mehreren Ländern tätigte. Das Bundeskriminalamt übernahm daraufhin den Fall.

„Soko Mozart". Da die Täter international vorgingen, wurde ein Treffen mit Ermittlern anderer Länder bei Europol organisiert; auf Betreiben des österreichischen Ermittlerteams und des zuständigen Staatsanwalts in Wien, Florian Kranz. „Unser Ziel war es, eine internationale Ermittlungsgruppe zu gründen, um die Täter auszuforschen, die nur unter ihren Nicknames im Internet bekannt gewesen sind", berichtet Chefinspektor Horst Hakala vom Bundeskriminalamt. 2013 wurde im Bundeskriminalamt die Ermittlungsgruppe „Soko Mozart" als Teil eines *Joint Investigationteams (JIT)* eingerichtet, dem weiters Ermittler aus Belgien, Finnland, Großbritannien und Norwegen angehörten. Später auch Ermittler aus den Niederlanden Es handelt sich um das größte gemeinsame Ermittlungsteam in der Geschichte von Eurojust/Europol. Das *JIT* steht unter der Leitung der Staatsanwaltschaft Wien und des Ermittlungsteams des österreichischen Bundeskriminalamts, das aus neun Spezialisten der Polizei besteht: erfahrenen Kriminalbeamten und IT-Experten. Die Bezeichnung „Mozart" wurde deshalb gewählt, weil die Ermittlungen in der „Mozart-Stadt" Salzburg ihren Anfang genommen hatten.

Verschleierte Kommunikation. Die Mitglieder der kriminellen Organisation nutzten bei der Kommunikation untereinander virtuelle private Netzwerke (VPN) und Proxy-Server, die die tatsächliche IP-Adresse der Täter verbargen. Die Ermittler der „Soko Mozart" konnten die Kommunikation der Kriminellen mitlesen. Sie hatten einander auf Russisch und Ukrainisch verständigt und benutzten Nicknames (Nicks), die keinen Bezug zu ihrer Identität hatten. Ihre Kommunikation wurde von Dolmetschern ins Deutsche übersetzt. Im Zuge der Ermittlungen wurde festgestellt, wer sich hinter welchem Nick verbarg. „Das war nicht leicht herauszufinden", sagt Hakala. Die Mitglieder der kriminellen Organisation kannten einander nicht persönlich. Es bestand lediglich Kontakt über die Nicks. Damit versuchten sie sicherzustellen, dass nicht alle Komplizen identifiziert werden können, sollte einer von ihnen ausgeforscht werden.

Kriminelle Hierarchie. Die kriminelle Organisation war wie ein Unternehmen aufgebaut. Die Ermittlungen der österreichischen Soko-Mitglieder richteten sich gegen den Kopf der Organisation. Ziel der Kriminellen war es, Geld von Konten von E-Banking-Nutzern auf andere Konten zu überweisen. Das konnte nur mit verteilten Rollen bewerkstelligt werden. Auf technischer Seite benötigte man Trojaner, um die Kontrolle über die PCs der Opfer zu erlangen, die zum Netbanking verwendet wurden. E-Banking-Nutzer „holten" sich die Malware durch das Öffnen schädlicher E-Mail-Anhänge oder von

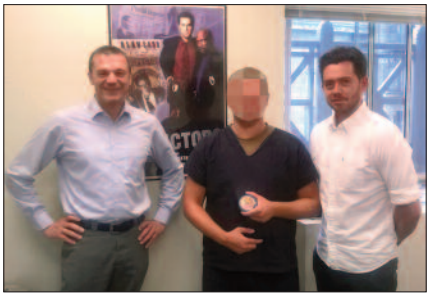
FOTO: BUNDESKRIMINALAMT

infizierten Webseiten. Für das Versenden von infizierten E-Mails wurden „Spammer“ eingesetzt. Der Trojaner wurde aktiv, sobald sich ein Nutzer in ein Netbanking-System eingeloggt hatte. „Dadurch konnten die Täter über die Internetverbindung des Opfers zur Bank dann von deren Konten Geld auf das Konto von Finanzagenten überweisen“, erläutert Soko-Leiter Hakala. Die „Finanzagenten“ wurden ebenfalls von „Spammern“ per E-Mail angeworben.

Finanzagenten. Der Kopf der kriminellen Organisation beauftragte seine Komplizen, Personen in ganz Europa für „Nebenjobs“ als „Finanzagenten“ anzuwerben. Diese wurden von den Kriminellen „Drops“ und von den Ermittlern „Money-Mules“ genannt. Die E-Mails, in denen für den „Nebenjob“ geworben wurde, erschienen auf den ersten Blick seriös. Als Absender schienen Firmen beispielsweise mit der Bezeichnung „Finance-Management“ auf. Die Kriminellen gaben vor, diese Firmen seien zum Beispiel für ein großes amerikanisches Unternehmen tätig, das in Europa Niederlassungen aufbauen wolle. Während der Aufbauphase benötige man einen „Finanzmanager“, der sein Konto für Geldüberweisungen nach Europa zur Verfügung stellte.

Die Tätergruppe verwendete mehr als 50 solcher „Firmen“ für die Rekrutierung der „Drops“. Die Kriminellen engagierten einen Grafiker, der die Webseite des amerikanischen Unternehmens nachbildete. Die Interessenten erhielten von der Rekrutierungsfirma einen Link der US-Firma zugesandt, für eventuelle Rückfragen. Der Link führte jedoch nicht zur echten Firma, sondern zu der nachgebildeten. Wer die Webseite anklickte, landete bei den Betrügern.

„Wer auf das Angebot eingestiegen ist, als „Finanzagent“ tätig zu werden, dem ist ein Werkvertrag zugesandt worden“, berichtet Hakala. Der „Finanzagent“ erhielt vier bis 20 Prozent des überwiesenen Geldbetrags. Er hatte den Auftrag, das Geld von seinem Konto zu beheben und über ein anonymes Geldtransfer-Unternehmen in die Ukraine zu überweisen. Die „Finanzagenten“ machten sich der Beteiligung an Geldwäsche strafbar. 55 solcher „Money Mules“ wurden in Österreich von den „Soko-Mozart“-Ermittlern bisher ausgeforscht. In den USA wurden die „Drops“ auch zum Weiterversand



Soko-Mozart-Ermittler Horst Hakala und Senan Moloney (Europol) mit dem in den USA festgenommenen Haupttäter der kriminellen Organisation.

von Paketen verleitet. In den Paketen waren Güter enthalten, die mit missbräuchlich verwendeten Kreditkartendaten oder gehackten Benutzerkontodaten gekauft worden waren. Da der Haupttäter über sämtliche „Arbeitsabläufe“ informiert werden wollte und stets Anweisungen an seine Komplizen gab, ließ er von IT-Experten eine Anwendung programmieren, die diese Abläufe automatisierte. Dieses System wurde als „Taskbot“ bezeichnet.

Geldflüsse. Die Polizei in den USA hatte schon längere Zeit gegen diese kriminelle Gruppe ermittelt, die dort vorwiegend betrügerisch erlangte Konsumartikel über „Paket-Agenten“ an Hehler weiterleitete. Die Ausforschung des Kopfes der Organisation, ein 28-jähriger Kasache, war nur aufgrund der Arbeit der österreichischen Ermittler möglich. „Es ist sehr schwierig gewesen, ihn ausfindig zu machen, denn er hat seine Aufenthaltsorte stets verschleiert – auch seinen Komplizen gegenüber“, berichtet Hakala. „Aufgrund seiner Verschleierungstaktik und des Umstandes, dass jeder Kriminelle dieser Organisation die Straftaten gegen österreichische Opfer von einem anderen Aufenthaltsort begangen hat, sind klassische Ermittlungsmethoden wie Tatortarbeit und Zeugenbefragung nicht möglich gewesen“, erläutert der Soko-Leiter.

Die Ermittler konnten einige wenige „Identifiers“ aus der Kommunikation der Täter herausfiltern, die letztlich zu deren Identifizierung führten. Der Haupttäter überwies seinen Komplizen deren Anteil auf Webmoney-Konten. „Es ist schwierig gewesen, den Geldfluss nachzuweisen“, sagt Hakala. Der Geldfluss wurde dem Haupttäter schließlich zum Verhängnis. Das Geld, das von den Konten der „Finanzagenten“ abgehoben und per Geldtransferdienste in die Ukraine transferiert worden war, tauchte auf einer ukrainischen Bank wieder auf. Ein Mittelsmann des Haupttäters hatte unter einer falschen Identität ein Konto eröffnet, auf das er das per Money-Transmitter in die Ukraine überwiesene Bargeld einzahlte. Er ließ sich mit der falschen Identität eine Kreditkarte ausstellen, kopierte die Informationen vom Magnetstreifen der Karte und übermittelte sie zusammen mit der dreistelligen Prüfziffer dem Haupttäter in die USA. Dieser kopierte die Magnetstreifen-Information auf seine echte, aber abgelaufene Kreditkarte und behob damit Geld an den Geldausgabeautomaten.

Aufgrund dieser und weiterer Informationen kamen die österreichischen Ermittler dem Haupttäter auf die Spur. Er wurde ausgeforscht und im Mai 2015 in Miami festgenommen. „Bei seiner ersten Einvernahme hat er gestanden, seit mindestens sieben Jahren diese Straftaten verübt und bis zu 250.000 US-Dollar wöchentlich gewaschen zu haben“, berichtet Hakala.

Festnahmen. Die Ermittler konnten elf weitere Mitglieder der kriminellen Organisation ausforschen. Im Juni 2015 schritten Polizisten in sechs Städten in der Ukraine gegen acht von ihnen ein. Ermittler der „Soko Mozart“ waren an den Polizeiaktionen leitend beteiligt. In der Ukraine war auch die sicherheitspolitische Lage in Betracht zu ziehen, „denn wir haben ja freiwillig an den Ermittlungen dort teilgenommen“, sagt Hakala.

Bei den Verdächtigen wurden 17 Terabyte digitalen Beweismaterials sichergestellt. Ein Server in den Niederlanden, den die Täter für ihre Geschäfte nutzten, wurde gesichert und nach gerichtlicher Weisung vom Netz genommen. „Der Haupttäter, der derzeit in den USA in Haft ist, hat sich vor einem amerikanischen Gericht für die von ihm und seiner Gruppe in Amerika begangenen Straftaten für schuldig erklärt“, sagt Hakala. „Die amerikanischen Ermittlungsbehörden gehen davon aus, dass sie ihm mehrere Tausend Straftaten mit einem Gesamtschaden in zweistelliger Millionenhöhe in US-Dollar nachweisen können.“

Die weiteren Mitglieder dieser Organisation wurden in der Ukraine inhaftiert und im Beisein von österreichischen Ermittlern einvernommen. Sie waren teilweise geständig. Der Tä-

FOTO: BUNDESKRIMINALAMT

tergruppe konnten bisher Straftaten in den USA, Spanien, den Niederlanden, Belgien, und Österreich nachgewiesen werden. Die Ermittler fanden Hinweise, dass die Täter auch in Griechenland, Frankreich, Italien, Großbritannien, Tschechien, Polen, Rumänien und Kroatien Straftaten begangen haben könnten. „Diese Beweismittel werden nach Abschluss der Ermittlungen diesen Ländern zur Verfügung gestellt“, betont Hakala.

Die Staatsanwaltschaft Wien hat 147 Anordnungen zu Kontoöffnungen, Hausdurchsuchungen und Sicherstellungen sowie sechs Festnahmeanordnungen und fünf europäische Haftbefehle erlassen. Der Ermittlungsakt umfasst 58 Aktenbände und ist 30.000 Seiten dick. Ermittelt wird wegen des Verdachts des betrügerischen Datenverarbeitungsmissbrauchs, der Mitgliedschaft in einer kriminellen Organisation, des schweren Betrugs und der Geldwäscherei. Einzelnen Verdächtigen droht eine Freiheitsstrafe bis zu zehn Jahren.

Das Strafverfahren in Österreich richtet sich gegen 55 Beschuldigte. Viele davon sind „Finanzagenten“, die ihre Konten für Überweisungen zur Verfügung stellten, ohne Bandenmitglieder zu sein. Darüber hinaus soll die Gruppe in Untergrundforen mit gestohlenen Anmeldedaten, kompromittierten Bankkontendaten und Malware gehandelt, Hacking-Dienste angeboten und nach neuen Partnern für ihre Cyber-Delikte gesucht haben.

„Die Ermittlungen gegen die kriminelle Organisation haben sich aufgrund der internationalen Tragweite schwierig und langwierig gestaltet“, sagt Soko-Leiter Hakala. Es wurden über 40 internationale Rechtshilfeersuchen an 20 Staaten gerichtet, um Erkenntnisse über die Identität der Täter zu gewinnen. „Bis jetzt sind noch nicht alle Antworten auf diese Ersuchen bei uns eingelangt“, sagt Hakala. „Aufgrund dieser Verzögerungen haben dringende Ermittlungen meist nur durch persönlichen Kontakt der Ermittler der einzelnen Staaten geführt werden können.“

Zur Koordinierung der internationalen Ermittlungen gab es acht Treffen bei Eurojust und 15 bei Europol in Den Haag. Es gab Arbeitsgespräche, Koordinierungs- und Einsatzbesprechungen in der Ukraine und in den USA. Im zweiwöchigen Takt wurden mit den ermittelnden Stellen Telefonkonferenzen durchgeführt, um den aktuellen Stand der Ermittlungen auszutauschen, etwaige Änderungen in der Taktik zu besprechen oder Einsatzzeiten zu koordinieren.

Festnahme eines Mitglieds der Cyber-Kriminellen in der Ukraine.

Internationale Anerkennung. Die Erfolge der Ermittlungen der „Soko Mozart“ als Teil eines Joint Investigationsteams mit so vielen Mitgliedsländern sind laut Europol/Eurojust einzigartig. Sie führten zu 60 Festnahmen in vier Staaten. „Die Mitarbeiter der Soko Mozart haben durch ihr Fachwissen, ihre hohe Motivation, ihre Einsatzbereitschaft und ihren Erfolg bei den Ermittlungen bewiesen, dass österreichische Ermittler jeden Vergleich mit Ermittlern anderer Staaten bestehen“, sagt Mag. Rudolf Unterköfler, Leiter der Abteilung 7 (Wirtschaftskriminalität) im Bundeskriminalamt. Vor der Arbeit der Experten der „Soko Mozart“ habe es laut Unterköfler in Österreich kaum Wissen über die Gliederung der kriminellen Struktur im Bereich des Internetbetrugs gegeben. Die Erkenntnisse der Ermittler werden in Schulungen anderen Ermittlern zugänglich gemacht.

Weltweit konnten aufgrund der Ermittlungen der Soko Hunderte Straftaten geklärt werden. Vor der Festnahme des Haupttäters in den USA präsentierte ein „Soko-Mozart“-Ermittler im Justizministerium in Washington die österreichischen Ermittlungsergebnisse vier Staatsanwälten, Mitarbeitern des FBI und des *United States Postal Inspection Service (USPIS)* sowie Europol-Mitarbeitern. Die USPIS-Mitarbeiter hatten bereits jahrelang erfolglos versucht, an die Hintermänner der Gruppierung zu gelangen, die für die „Paket-Agenten“ verantwortlich waren. Der Fall wurde auch in Pittsburgh bei einer Konferenz 40 FBI-Agenten zu Schulungszwecken präsentiert.

„Dieser Fall zeigt, dass der erfolgreiche und nachhaltige Kampf gegen Cyber-Kriminalität nur möglich ist, wenn alle Beteiligten grenzübergreifend koordinieren und kooperieren“, betont Ingrid Maschl-Clausen, die österreichische Vertreterin bei Eurojust.

Der Fall ist noch nicht abgeschlossen: Die Durchsicht des gesamten Beweismaterials dürfte Monate dauern, Ermittlungen zu weiteren Mitgliedern der Organisation laufen. „In den sichergestellten Beweismitteln finden sich Hinweise, die zur Klärung weiterer, vermutlich Tausender Straftaten weltweit führen werden“, sagt Hakala. „Der Erfolg der Soko Mozart ist letztendlich nur aufgrund der hervorragenden Zusammenarbeit jedes einzelnen Team-Mitglieds möglich gewesen“, betont Hakala. „Wir sind vielen Hinweisen nachgegangen und dabei oft ins Leere getappt, weil der Haupttäter falsche Informationen gestreut hat“, berichtet Hakala. „Es ist schwierig gewesen, aus den Chats brauchbare Informationen herauszufiltern. Doch Hartnäckigkeit und Genauigkeit haben sich bezahlt gemacht.“ *Siegbert Lattacher*

JIT

Soko „Mozart“ und Partner

An den von Österreich eingeleiteten Ermittlungen gegen die kriminelle Organisation waren beteiligt: Cybercrime Division Ukraine, FBI Field Office New York, United States Postal Inspection Service (USPIS), High Tech Crime Team Niederlande, Internet Investigation Team Belgien, National Bureau of Investigation Finnland, Police Central e-crime Unit Großbritannien, High-Tech-Crime-Team-Norwegen, Cyber Crime Center (EC3) von Europol, „Soko Mozart“ Österreich.

FOTO: BUNDESKRIMINALAMT