Bundeskriminalamt

BKA

FIU-Newsletter

- 13. Ausgabe -

Juni 2016

Inhalt

A Einleitung

Sehr geehrte Damen und Herren,

ich freue mich, Ihnen die 13. Ausgabe des Newsletters der Financial Intelligence Unit (FIU) Deutschland vorstellen zu können.

Das Hauptthema des aktuellen Newsletters ist der sogenannte „CEO-Fraud“. Dies ist eine neue Betrugsvariante, bei der Unbekannte die Mitarbeiter eines Unternehmens kontaktieren, sich diesen gegenüber als Vertreter der Geschäftsleitung ausgeben und diese zu nicht legitimierten Zahlungen ins Ausland veranlassen. Der Newsletter enthält zudem neben Hintergrundinformationen zu diesem Phänomen auch Fallbeispiele und eine Auflistung verdachtserregender Momente.

Im Teil C wird ein neuer Modus Operandi anhand eines Fallbeispiels beschrieben, der im Zusammenhang mit fingierten Kaufabwicklungen und dem Einsatz von Geschenkgutscheinen/Coupons von Online-Verkaufsplattformen durchgeführt wurde.

Im Teil D „Sonstiges“ sind neben einem Fallbeispiel zu einer neuen Variante der Anwerbung eines „Finanzagenten“ über ein Partnervermittlungsportal noch allgemeine Hinweise zum Postidentverfahren enthalten.

Ich hoffe, dass auch der aktuelle Newsletter eine hilfreiche Ergänzung im Rahmen der Wahrnehmung Ihrer gesetzlichen Pflichten ist.

Mit freundlichen Grüßen

Dr. Michael Dewald (Leiter FIU Deutschland)

B CEO-Fraud

I. Vorbemerkung

In den vergangen Monaten ist eine Vielzahl von deutschen Firmen Opfer des sog. CEO-Fraud geworden. Diese erlitten dabei zum Teil Verluste in Millionenhöhe. Die nachfolgenden Hinweise und Beispiele sollen den Verpflichteten eine Hilfestellung bieten, ihre Kunden vor derartigen Betrügereien zu schützen, die Transaktionen vor Durchführung abzuklären und Hinweise auf diese Betrugsvariante an den Kunden weiterzugeben.

II. Warnhinweise zum CEO-Fraud

Beim CEO-Fraud geben sich Täter - nach Sammlung jeglicher Art von Information über das „anzugreifende“ Unternehmen - beispielsweise als Geschäftsführer (CEO) oder als Teil der Geschäftsführung des Unternehmens aus und veranlassen einen Unternehmensmitarbeiter zum Transfer eines größeren Geldbetrages an einen nicht autorisierten Empfänger zumeist ins Ausland.

Die Täter nutzen hierfür Informationen, die Unternehmen in Wirtschaftsberichten, im Handelsregister, auf ihrer Homepage oder in Werbebroschüren veröffentlichen. Die Täter legen ihr Augenmerk insbesondere auf Angaben zu Geschäftspartnern und künftigen Investments. Für die Betrüger sind beispielsweise E-Mail-Erreichbarkeiten von Interesse, da sie daraus die Systematik von Erreichbarkeiten herleiten. Soziale Netzwerke, in denen Mitarbeiter ihre Funktion und Tätigkeit oder persönliche Details preisgeben, stellen ebenfalls eine wichtige Informationsquelle dar.

Auf diese Weise verschaffen sich die Täter das für den Betrug notwendige Insiderwissen über das betreffende Unternehmen.

Die Täter nehmen in einem weiteren Schritt mit dem "ausgeforschten" Mitarbeiter Kontakt auf und geben sich als leitende Angestellte, Geschäftsführer oder Handelspartner aus. Dabei fordern sie z.B. unter Hinweis auf eine angebliche Unternehmensübernahme oder angeblich

geänderte Kontoverbindungen den Transfer eines größeren Geldbetrages auf hauptsächlich ausländische Konten, die beispielsweise bei Banken in China und Hong Kong, aber auch in osteuropäischen Staaten geführt werden.

Die Kontaktaufnahme erfolgt in der Regel über E-Mail oder Telefon, wobei E-Mail-Adressen verfälscht und Telefonnummern verschleiert werden.

Durch CEO-Fraud konnten Kriminelle in den letzten Monaten bereits mehrere Millionen Euro mit zum Teil gravierenden Folgen für die betroffenen Unternehmen bzw. die getäuschten Mitarbeiter erbeuten. In einer Vielzahl von Fällen waren die Täter jedoch nicht erfolgreich, weil die kontaktierten Mitarbeiter aufmerksam waren und sich von den professionell vorgehenden Tätern nicht täuschen ließen.

Zum Schutz vor der Betrugsmasche rät die Polizei:

- Achten Sie darauf, welche Informationen über Ihr Unternehmen öffentlich sind bzw. wo und was Sie und Ihre Mitarbeiter im Zusammenhang mit Ihrem Unternehmen publizieren!
- Führen Sie klare Abwesenheitsregelungen und interne Kontrollmechanismen ein!
- Sensibilisieren Sie Ihre Mitarbeiter hinsichtlich des beschriebenen Betrugsphänomens
- Bei ungewöhnlichen Zahlungsanweisungen sollten vor Veranlassung der Zahlung folgende Schritte durchgeführt werden:
    - Überprüfen der E-Mails auf Absenderadresse und korrekte Schreibweise
    - Verifizieren der Zahlungsaufforderung über Rückruf bzw. schriftliche Rückfrage beim Auftraggeber
    - Kontaktaufnahme mit der Geschäftsleitung bzw. dem Vorgesetzten

- Wenden Sie sich bei Auffälligkeiten und Fragen an die örtliche Polizeidienststelle oder an das zuständige LKA!

Veröffentlichungen des Warnhinweises:

- http://www.bka.de/nn_206064/DE/ThemenABisZ/Kriminalpraevention/Warnhinweise/151223__CEOBetrug.html

- http://www.polizei-beratung.de/startseite-und-aktionen/aktuelles.html)

III. Fallbeispiele zum CEO-Fraud

Fall 1:

Ein Mitarbeiter der Buchhaltung eines mittelständischen Unternehmens wird vom angeblichen Geschäftsführer seiner Firma per E-Mail kontaktiert und angewiesen, für die Übernahme eines anderen Unternehmens mehrere streng vertrauliche Geldtransfers ins Ausland durchzuführen. Für die Details der Zahlungen sei eine Rechtsanwaltskanzlei in Luxemburg zuständig, die sich in der Folge sowohl per E-Mail als auch telefonisch mit dem Mitarbeiter in Verbindung setzt und entsprechende Rechnungen in Höhe von insgesamt 1,5 Mio. EUR übermittelt. Da der Mitarbeiter des Unternehmens für die Zahlung dieser Summen alleine keine Berechtigung hat, involviert er eine weitere Buchhalterin im Unternehmen. Nachdem sich beide Buchhalter über die Existenz der Anwaltskanzlei im Internet informiert haben, führen sie die Zahlungen, die auf Konten in China und Hong Kong gehen, durch. Im Nachhinein stellt sich heraus, dass Name und Erreichbarkeiten der Anwaltskanzlei zur Begehung des Betruges missbräuchlich verwendet wurden.

Fall 2:

Ein Anrufer (Telefonnummer unterdrückt), der sich als Verantwortlicher einer bekannten Unternehmensberatung A vorstellt, weist mit dem Wissen, dass der Geschäftsführer der Firma B abwesend ist, eine Mitarbeiterin der Firma B an, einen Betrag i.H.v. ca. einer Million EUR für einen Firmenkauf zu überweisen. Dies sei so mit dem Geschäftsführer der Firma B

abgesprochen. Hierzu werden durch den Betrüger gefälschte E-Mails, die angeblich vom Geschäftsführer der Firma B stammen, vorgelegt. Zur Bestätigung der Überweisung solle der Überweisungsträger in Kopie an die E-Mail-Adresse des Verantwortlichen der Unternehmensberatung A übersandt werden. Begünstigter der Überweisung solle eine Firma C mit Sitz und Bankverbindung in China sein. Da die angerufene Mitarbeiterin aber mit ihrem Geschäftsführer Kontakt aufnimmt, kann der Betrug verhindert werden. Im Nachhinein stellt sich heraus, dass der Name der Unternehmensberatung zur Begehung des Betruges missbräuchlich verwendet wurde.

Fall 3:

Firma X aus Deutschland unterhält seit mehr als 20 Jahren Geschäftsbeziehungen zu Firma Y in Hong Kong. Es wird zwischen den beiden Firmen eine Bestellung von Textilartikeln vereinbart. Die angeforderte Sendung wird von Firma Y in Hong Kong auf den Seeweg gebracht. Im Anschluss erhält Firma X in Deutschland über die bekannte E-Mail-Adresse der Firma Y aus Hong Kong die Information, dass es eine Änderung der Bankverbindung gegeben habe und die Rechnung auf ein neues Firmenkonto bei einer Bank in China zu überweisen sei.

Aus diesem Grund überweist die Buchhalterin der Firma X in Deutschland die geforderte Rechnungssumme in Höhe von über 130.000,- USD ohne Argwohn auf das neue Konto. In einem danach geführten Telefongespräch erklärt Firma Y in Hong Kong, dass kein Zahlungseingang zur oben genannten Bestellung verzeichnet werden konnte. Auf Nachfrage erklärt sie außerdem, dass keine neue Bankverbindung eingerichtet und auch keine entsprechende E-Mail mit einer Veränderungsinformation versandt worden sei.

Verdachtserregende Momente bei derartigen Fallkonstellationen:

- Transaktion im mindestens 6-stelligen Bereich, häufig sogar mehrere Mio. Euro

- Absender: eine in Deutschland ansässige Firma mit Konto bei einer Bank in Deutschland

- Empfänger: Konto/Firma im Ausland, vornehmlich in China oder Hong Kong, aber auch in osteuropäischen Staaten

- Eilbedürftige Transaktion (z. B. vor dem Wochenende) unter Hinweis auf Vertraulichkeit/Geheimhaltungserfordernis

- Besonderheit: Transaktionen auf dieses Empfängerkonto fanden durch die Firma in Deutschland bisher nicht statt

C Neuer Modus Operandi

I. Fallbeispiel

Im Rahmen eines Ermittlungsverfahrens gegen Betreiber und Mitglieder von sog. Underground Economy-Foren (UE-Foren) wurde eine möglicherweise neuartige Methode zur Geldwäsche von illegalen Gewinnen durch das Einlösen von Gutscheincodes bei Online-Verkaufsplattformen (hier am Beispiel Amazon) festgestellt. Die Täter betrieben eine illegale Streaming-Plattform, über die insbesondere die Inhalte des Pay-TV-Senders SKY angeboten und gegen die Zahlung monatlicher Gebühren zugänglich gemacht wurden. Diese Gebühren ließen sich die Täter in Form von Gutscheincodes der Firma Amazon bezahlen.

Über die Handelsplattform wurden dann mittels fingierter Kaufabwicklungen die inkriminierten Gelder „rein gewaschen“ und die Täter verfügten so am Ende über eine Gutschrift auf ihrem Bankkonto seitens der Firma Amazon.

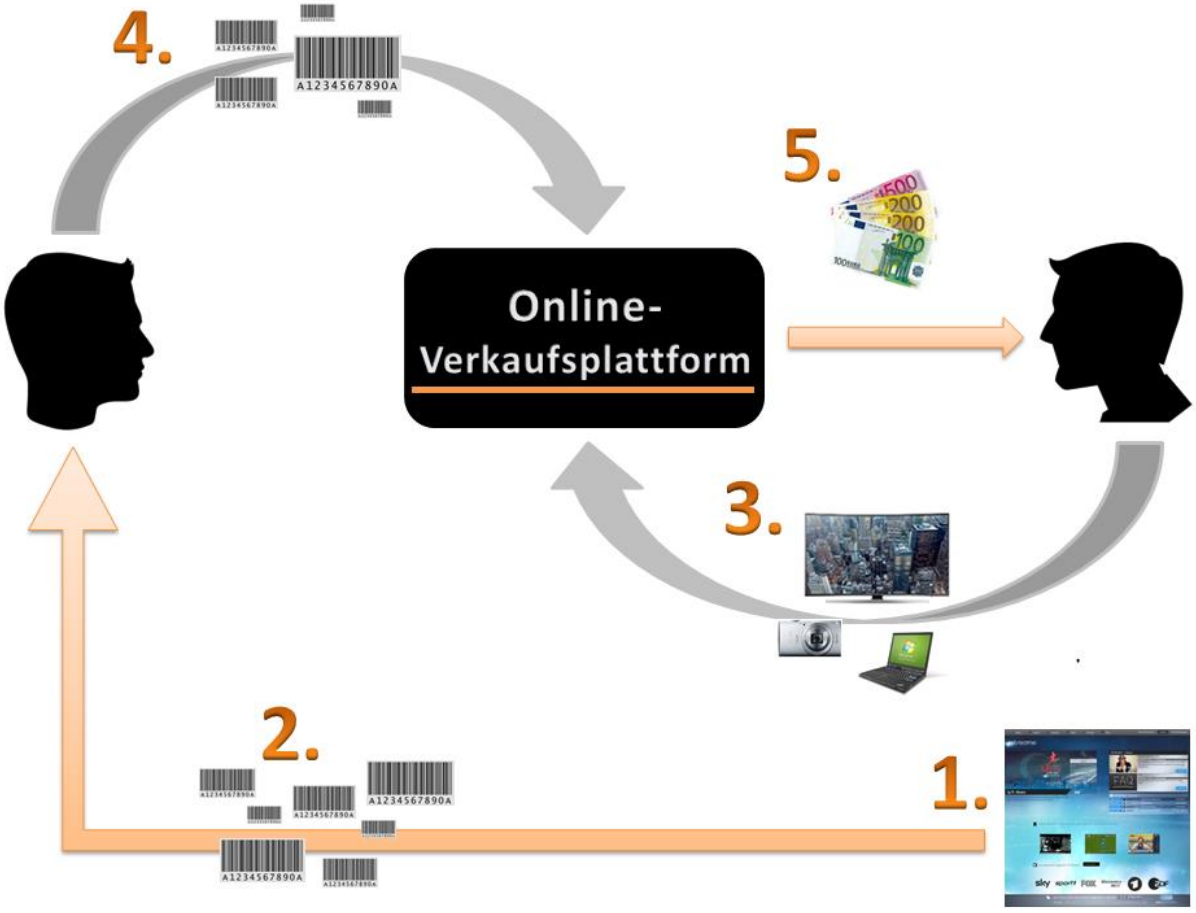
Auf der Online-Plattform Amazon wurden zunächst auf einem legitimen Konto hochpreisige Elektronikartikel eingestellt und im Anschluss durch ein weiteres betrügerisch eingerichtetes Kundenkonto die zuvor eingestellten Artikel gekauft.

Die eingestellten Artikel waren nicht existent. Die Beschuldigten hatten auf dem zweiten Konto im Vorfeld der Kaufabwicklung massenhaft die Gutscheincodes hinterlegt. Die so „legalisierten“ Einnahmen bewegten sich im sechsstelligen Euro-Bereich.

Durch fingierte Verkäufe können so in der Summe hohe illegale Geldbeträge in den legalen Wirtschaftskreislauf eingeführt und damit „gewaschen“ werden. Die massenhaften Einlösungen bzw. Verwendungen von Gutscheincodes führen somit dazu, dass Online-Handelsplattformen unfreiwillig als Plattform zur Geldwäsche genutzt werden. Einen entsprechenden Erkennungsmechanismus seitens der Handelsplattformen scheint es zumindest bei der Fa. Amazon bislang nicht zu geben.

II. Neuer Modus Operandi

Nachfolgend wird der neue festgestellte Modus Operandi „Geldwäsche mittels Gutscheincodes über Online-Verkaufsplattformen“ dargestellt:



Geldwäschevorgang:

1. Erzielung von Einkünften in Form von Gutscheincodes für eine Online-Handelsplattform aus illegalen Aktivitäten innerhalb der Underground Economy.

2. Einlösung (Hinterlegung) der Gutscheincodes auf einem (kompromittierten/unter Falschpersonalien eingerichteten oder anderweitig anonymisierten) Käuferkonto bei der Online-Handelsplattform

3. Einstellung von Angeboten nicht existenter Waren über ein weiteres legitimes Verkäuferkonto

4. Bezahlung der eingestellten Waren mittels der eingelösten Gutscheine über das Käuferkonto

5. Verkäufer erhält den Kaufpreis als Gutschrift von der Online-Handelsplattform aufgrund der getätigten Kaufabwicklung auf sein hinterlegtes Bankkonto

D Sonstiges

Finanzagent statt Partneranbahnung

Über ein Partnervermittlungsportal nahm eine Tätergruppierung Kontakt zu einer männlichen Person auf. Von der weiblichen Person mit afrikanisch klingendem Namen wurde eine gewünschte Beziehung vorgespielt. Das männliche Opfer wurde in der Folge dazu bewegt, Gelder nach Nigeria zu überweisen, um der „Partnerin“ eine Reise nach Deutschland zu finanzieren.

Im weiteren Verlauf der „Beziehung“ wurde zudem vorgetäuscht, dass die Frau im Besitz eines Anlagefonds sei, für dessen Auszahlungsreife noch Zahlungen notwendig seien. Diese Zahlungen wurden aus verschiedenen Ländern nahezu sämtlicher Kontinente erwartet. Das „männliche Opfer“ wurde ebenfalls dazu bewegt, einen sechsstelligen Eurobetrag auf den Anlagefonds zu überweisen. Zudem erhielt der Mann seinerseits einen geringeren sechsstelligen Betrag auf sein Konto und wurde angewiesen, diesen ins Ausland weiter zu überweisen. Nachdem er selbst erst um einen hohen Geldbetrag betrogen wurde, ließ er sich anschließend als „Finanzagent“ anwerben und machte sich damit möglicherweise strafbar.

Ein führendes Mitglied der Tätergruppierung ließ sich einmal auf sein legales Konto von dem Opfer Geld überweisen und reiste zur Entgegennahme der letzten fünfstelligen Summe eigens aus dem Ausland nach Deutschland ein.

Die Täter wurden bei der Geldübergabe festgenommen. Ausgangspunkt der Ermittlungen waren mehrere Verdachtsmeldungen.

Verdachtserregende Anhaltspunkte:

- Nicht zum Kundenprofil passendes Transaktionsverhalten
- Ungewöhnliche Zahlungseingänge aus dem Ausland

- Ungewöhnliche Zahlungen ins Ausland per Überweisung und via Finanzdienstleister
- Zahlungseingänge mit direkt anschließendem Weitertransfer oder Barauszahlungen

Ausweiskopien im Postidentverfahren

Aufgrund der mittlerweile zahlreichen unterschiedlichen Legitimationspapiere, die zur Eröffnung von Bankkonten akzeptiert werden, hat sich bei der Deutschen Post in Bezug auf das Postidentverfahren eine Neuerung ergeben.

Eröffnen Kunden online bei einer Bank ein Konto und legitimieren sich daraufhin im Rahmen des Postidentverfahrens, so wird seit Mitte November 2015 eine Ausweiskopie seitens der Postfiliale gefertigt und eingescannt. Bislang wurden keine Kopien aufbewahrt.

Über das Auskunftsportal der Deutschen Post haben die Auftraggeber – die Kreditinstitute – die Möglichkeit, sich binnen 72 Stunden diese Ausweiskopien herunter zu laden. Danach werden die Ausweiskopien unwiderruflich gelöscht.

Die Kreditinstitute haben so die Möglichkeit, innerhalb dieser Frist die Kundendaten zu überprüfen und festzustellen, mit welchem Ausweisdokument sich der jeweilige Kunde legitimiert hat.

Kontakt

Für Kontaktaufnahmen stehen wir Ihnen gerne unter den nachfolgenden Erreichbarkeiten zur Verfügung.

Bundeskriminalamt

Referat SO 32 - FIU

Zentralstelle für Verdachtsmeldungen

65173 Wiesbaden

Fax: +49-(0)611-55 45300

E-Mail: FIU@bka.bund.de

Impressum:
Bundeskriminalamt
Referat SO 32 - FIU
Zentralstelle für Verdachtsmeldungen
65173 Wiesbaden
Fax: +49-(0)611-55 45300
E-Mail: FIU@bka.bund.de