/ Lücken und Tücken beim aktuellen Problem des Cyber-CEO Fraud

29.05.2017

Gesellschaftsrecht/Mergers & Acquisitions | Compliance & Interne Ermittlungen

1. Problemabriss

Sowohl das Bundeskriminalamt als auch mehrere internationale Banken haben in den letzten Monaten zahlreiche Warn- und Schutzhinweise zum aktuellen Problem des sog. CEO Fraud (auch Chef Betrug, Geschäftsführerschwindel oder "Business E-Mail Compromise" (BEC) genannt) veröffentlicht. Bei dieser modernen Form des "Cybertrickbetruges" kontaktiert ein sich als Geschäftsführer, Vorstandsmitglied oder sonstiger leitender Angestellter ausgebender Dritter einen über längere Zeit hinweg ausgespähten Mitarbeiter (z.B. Buchhalter, Heimleiter), der unverzüglich eine "äußerst vertrauliche" Onlineüberweisung ausführen müsse. Nachdem die Täter sodann das Vertrauen des Mitarbeiters gewonnen haben, veranlasst dieser – in der Regel arglos auf die vermeintlich legitime Anweisung des falschen Vorgesetzten – die Transaktion, oftmals in Millionenhöhe, auf ein ausländisches Konto. Problematisch ist dies vor allem dann, wenn die ausführende Bank die Überweisung nicht mehr stoppen kann, etwa weil der Betrag dem Konto bei der Empfängerbank bereits gutgeschrieben wurde.

2. Manipulationsstrategien und Informationsbeschaffung der Täter

Typisches Vorgehen der Trickbetrüger

Üblicherweise nehmen die meist im Ausland sitzenden (Haupt-)Täter erstmals mittels E-Mail Kontakt auf, in welcher der vermeintliche Chef wegen einer "äußerst wichtigen, streng geheimen Unternehmenstransaktion" die Überweisung eines mehrstelligen Geldbetrages ins Ausland wünscht. Dass die Absender-Adresse zwar den richtigen Namen des CEO nennt, der Endabschnitt jedoch nicht dem firmeninternen E-Mail-Provider entspricht bzw. sich lediglich durch einen Buchstaben unterscheidet, wird dabei schnell übersehen. Sofern der Mitarbeiter nach vorgeschobenen Schmeicheleien, z.B. über dessen hohe Vertrauenswürdigkeit und Diskretion immer noch zaudert, kontaktiert nicht selten ein – sich als Berater einer bekannten Kanzlei ausgebender, eloquenter – "Anwalt" diesen nochmals telefonisch, um letzte Zweifel "auszumerzen". Jene Betrugsmasche ist jedoch letztlich nur deshalb so oft von Erfolg gekrönt, weil die Täter umfangreiche Kenntnisse vom Unternehmen und dem angesprochenen Mitarbeiter haben. Dahingehende Informationen verschaffen sich diese in der Regel leicht über das Internet.

Frei verfügbare Online-Daten

Unternehmensrelevante Auskünfte wie die aktuelle Wirtschaftslage, Struktur und Führungsebene sowie Geschäftspartner, Investoren und Mitarbeiter erhalten die Täter in erster Line über digitale Plattformen. Neben bekannten "Datenkraken" zählt hierzu das elektronische Unternehmensregister, in dem Jahresabschlüsse der Gesellschaft offengelegt sind, sowie das Handelsregister, indem Beschlüsse der Investoren hinterlegt sind, welche von jedermann und ohne Angabe berechtigter Interessen beim Registergericht elektronisch abgefragt werden können. Hinzukommen Online-Portale, welche aktuelle Investitionen und regelmäßig mandatierte Kanzleien des Unternehmens preisgeben. Eine weitere wichtige Informationsquelle der Täter ist auch die Unternehmenswebsite, welche die Kontaktdaten der Vorgesetzten und mitunter der Buchabteilung ausweist. Schließlich erlangen die Täter Kenntnis vom relevanten Unternehmenspersonal über soziale Netzwerke, etwa solche, die der Pflege von Geschäftskontakten dienen. Aus diesen ergeben sich Funktion und Tätigkeitsschwerpunkte der Mitarbeiter. Die Informationsquellen der Täter sind jedoch letzten Endes vielfältig und daher nicht abschließend bestimmbar, weshalb umso mehr das Bewusstsein aller Mitarbeiter im Unternehmen um die Gefahren des CEO Fraud geschärft werden sollte.

3. Maßnahmen zur Sicherung des Geldbetrages im Ausland und Rücküberweisung

Doch was ist zu tun, wenn die Überweisung bereits getätigt wurde?

- **Unverzügliche Kontaktaufnahme mit den beteiligten Banken**

  Sobald der fälschlicherweise überwiesene Geldbetrag auf das Konto der ausländischen Empfängerbank überwiesen und diesem gutgeschrieben wurde, ist ein "Zurückholen" durch die ausführende deutsche Bank in der Regel kaum mehr möglich. Aus deutscher Perspektive scheidet ein Anspruch auf Wiedergutschrift (§ 675u S. 2 BGB) bereits aus, wenn die Überweisung ein autorisierter Zahlungsvorgang nach § 675j Abs. 1 BGB ist. Das Gleiche gilt für einen Widerruf nach § 675p BGB, sofern nach Abs. 4 BGB nicht etwas anderes vereinbart wurde. Eine entsprechende Kontaktaufnahme sowohl mit der ausführenden Bank als auch der Empfängerbank ist dennoch sinnvoll, vor allem um diese zum Mitwirken beim Procedere der Rücküberweisung zu sensibilisieren. Eine sofortige Rücküberweisung durch die ausländische Bank ohne rechtskräftigen Beschluss einer staatlichen Institution dürfte jedoch unwahrscheinlich sein, insbesondere wenn es sich nicht um ein mit der ausführenden Bank verbundenes Unternehmen handelt.

- **Sofortiges Einschalten der deutschen und ausländischen Staatsanwaltschaft**

  Das vorrangige Ziel ist es demnach, den Tätern den Zugriff auf den Geldbetrag im Ausland bis zur Rücküberweisung schnellst möglich zu "versperren". Mittels Strafanzeige bei der zuständigen Staatsanwaltschaft sowohl in Deutschland als auch im Ausland lässt sich bei der ausländischen Behörde nicht selten der Erlass eines dem deutschen dinglichen Arrest entsprechenden Sicherungsmittels erwirken. Dagegen kann die deutsche Staatsanwaltschaft im Ausland (nur) einen dahingehenden Rechtshilfegesuch stellen, dessen Erfolg aber letztlich offen bleibt. Gleichwohl können deren Ermittlungen in das ausländische Strafverfahren positiv einfließen und damit den Rücküberweisungsprozess erheblich beschleunigen.

- **Rückabwicklung am Beispiel einer irrtümlichen Überweisung auf ein polnisches Konto**

  Um die im polnischen Recht verankerten effizienten Schutzmaßnahmen bei einer durch einen CEO Fraud verursachten Falschüberweisung auf ein polnisches Bankkonto effektiv auszuschöpfen, empfiehlt sich als ersten Schritt, schnellstmöglich über die ausführende deutsche Bank Kontakt mit der polnischen Empfängerbank aufzunehmen, um diese über den Betrugsfall zu informieren und das Risiko der Abhebung oder Weiterüberweisung des Geldbetrages auszuschließen.

  - *Sperrung des Bankkontos durch Empfängerbank und Staatsanwaltschaft*

  Im Prinzip ist jedes in Polen tätige Finanzinstitut verpflichtet, alle aus dem Ausland stammenden Transaktionen über EUR 15.000 oder bei denen nach den Umständen des Einzelfalls Hinweise bestehen, dass sie im Zusammenhang mit einer Straftat stehen (z.B. Geldwäsche, Finanzierung von Terrorismus), zu registrieren und dem Generalinspektor für Finanzielle Information mitzuteilen (Generalny Inspektor Informacji Finansowej). Bei einem begründeten Verdacht ist die polnische Empfängerbank zudem berechtigt, die Geldmittel bis zu höchstens 72 Stunden vor dem Zugriff des Kontoinhabers zu sperren. In der Regel erfolgt dies bereits dann, wenn die Empfängerbank von der ausländischen (deutschen) Bank über den Verdacht des Betrugs informiert wird. Parallel hierzu ist unverzüglich die zuständige polnische Staatsanwalt über den Vorfall zu informieren, welche binnen vorgenannter 72 Stunden einen Beschluss über die Einleitung eines strafrechtlichen Verfahrens erlassen kann. Im Falle dessen kann diese die Kontosperrung für höchstens 3 Monate ab dem Eingang der Anzeige verlängern.

  - *Antrag auf Rücküberweisung bei der polnischen Staatsanwaltschaft*

  Für den Geschädigte empfiehlt sich, bei der Empfängerbank um Auskunft über die zuständige Staatsanwaltschaft, inkl. Aktenzeichen zu ersuchen und sich dem Ermittlungsverfahren vor dem Ablauf der 3-monatigen Kontosperrfrist anzuschließen. Sofern Anhaltspunkte für eine Überweisung ohne Rechtsgrund bestehen, kann die Staatsanwaltschaft bei entsprechender Antragstellung einen Beschluss erlassen, in dem sie die Entsperrung des Bankkontos und die zeitgleiche Rücküberweisung des Betrags auf das Konto des Geschädigten anordnet. Eine zwischenzeitliche Überweisung auf ein Treuhandkonto der Empfängerbank zwischen der Kontoentsperrung und der Rücküberweisung ist daher nicht zwingend.

- Rechtskraft ab Zustellung an alle beteiligten Parteien

Beschlüsse der polnischen Staatsanwaltschaft sind grundsätzlich nach Eintritt der Rechtskraft ausführbar, d.h. nach Ablauf von 7 Tagen ab Zustellung an alle Beteiligten (mithin die polnische Empfängerbank, den Geschädigten bzw. dessen Bevollmächtigten und den Kontoinhaber). Problematisch ist, dass beim CEO-Fraud der Kontoinhaber oftmals eine Briefkastenfirma ist, im Falle dessen die Zustellung des Beschlusses durch Niederlegung im „Briefkasten" beim zuständigen Postamt erfolgt. Insofern gilt der Beschluss erst nach 14 Tagen als zugestellt, was die Rücküberweisung um diesen Zeitraum verzögert.

- Enge Kommunikation mit der Empfängerbank nach Beschlussfassung

Weiterhin empfehlenswert ist, bereits ab Beschlussfassung mit der zuständigen polnischen Bank im besonders engen Kontakt zu stehen, um sicherzustellen, dass die Geldmittel nach Ablauf der 3-monatigen staatsanwaltschaftlichen Sperrfrist und vor Eintritt der Rechtskraft des Beschlusses nicht durch den Kontoinhaber abgehoben, an weitere Banken überwiesen oder anderweitig transferiert werden. Sollte die Bank entgegen der staatsanwaltschaftlichen Anordnung eine Verfügung über den Geldbetrag durch die Täter dennoch zulassen und somit nicht mehr in der Lage sein, das Geld an den Geschädigten nach Eintritt der Rechtskraft des Beschlusses zurück zu überweisen, setzt sie sich dem Risiko eines Schadensersatzanspruches aus.

4. Hinweis für die Praxis – Ausbau eines effektiven Compliance-Systems

Wie beim sog. "Enkel-Trick-Betrug" nutzen die Täter allgemein bekannte Schwächen aus. Bei Unternehmen handelt es sich hierbei oftmals um ein eher starres Hierarchieverständnis, Ängste der Mitarbeiter vor dem Chef, den man im Zweifel nur aus dem Vorstellungsgespräch (wenn überhaupt) kennt, weshalb telefonische Rückfragen trotz evidenter Bedenken unterbleiben, und/oder eine nicht selten antiquierte Unternehmenskultur ohne umfangreiche, effektive Compliance-Regelungen. Dies ist nicht selten Existenz bedrohend. Im Zeitalter der stetig ansteigenden organisierten Cyberkriminalität ist daher eine rechtlich fundierte Beratung zur Etablierung eines funktionsfähigen Compliance-Systems wichtiger denn je.

Haben Sie Fragen? Kontaktieren Sie gerne: Dr. Romy Nicole Fleischer oder Maciej Gorgol
Practice Group: Gesellschaftsrecht/Mergers & Acquisitions und Compliance & Interne Ermittlungen

Contact Person

Dr. Romy Nicole Fleischer
Mitglied der Practice Group Gesellschaftsrecht/Mergers & Acquisitions
Rechtsanwältin

T +49 351 8166029

Maciej Gorgol
Mitglied der Practice Group Gesellschaftsrecht/Mergers & Acquisitions
Adwokat

T +48 22 3957663