

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/innen im Zusammenhang mit Ihrem Unternehmen publizieren!
- Führen Sie **klare Abwesenheitsregelungen** und **interne Kontrollmechanismen** ein!
- **Sensibilisieren Sie Ihre Mitarbeiter/innen** hinsichtlich des beschriebenen Betrugsphänomens!
- Bei **ungewöhnlichen Zahlungsanweisungen** sollten - vor Veranlassung der Zahlung - **folgende Schritte** durchgeführt werden:

1. **Überprüfen der E-Mails**
auf Absenderadresse und
korrekte Schreibweise

2. **Verifizieren der Zahlungsaufforderung** über Rückruf bzw. schriftliche Rückfrage beim genannten Auftraggeber

3. **Kontaktaufnahme mit der Geschäftsleitung bzw. dem Vorgesetzten**

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

KONTAKT

Landeskriminalamt NRW
Völklinger Str. 49
40221 Düsseldorf

Zentrale Ansprechstelle Cybercrime (SPoC)
Telefon +49 211 939 -4040
Fax +49 211 939 4198



Bundeskriminalamt



POLIZEI
Nordrhein-Westfalen
Landeskriminalamt



CEO-Fraud Warnhinweis

Warnung vor Betrugsmasche zum Nachteil von Unternehmen:

Beim **CEO-Fraud** geben sich **Täter** - nach Sammlung jeglicher Art von Information über das anzugreifende Unternehmen - beispielsweise als **Geschäftsführer** (CEO) des Unternehmens aus und veranlassen einen Unternehmensmitarbeiter zum **Transfer eines größeren Geldbetrages ins Ausland**.

Tatvorbereitung

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 Täter 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.

Tatbegehung

Die Täter nehmen mit den „ausgeforschten“ Mitarbeitern 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 geänderter Kontoverbindungen den **Transfer eines größeren Geldbetrages auf Konten in China und Hong Kong**, aber auch in osteuropäischen Staaten. Die **Kontaktaufnahme** erfolgt in der Regel über **E-Mail** oder **Telefon**, wobei E-Mail-Adressen verfälscht und Telefonnummern verschleiert werden.

Schäden

Durch **CEO-Fraud** konnten Kriminelle in den letzten Monaten bereits **mehrere Millionen Euro** mit zum Teil gravierenden Folgen für das betroffene 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.

