CEO Fraud in vier Akten

Internet-Betrug mit vorgetäuschten Identitäten

5.06.19 | Autor / Redakteur: Dietrich W. Thielenhaus / Peter Schmitz

Unternehmen sind immer öfter dem Risiko ausgesetzt, Opfer eines CEO-Fraud zu werden. (Bild: gemeinfrei / Pixabay)

Eine neue Form des Internet-Betrugs breitet sich auch in Deutschland aus, der CEO Fraud. Dabei geben sich international vernetzte Banden als Vorgesetzte aus und manipulieren Firmenmitarbeiter – oft äußerst raffiniert – zu objektiv unbegründeten Auslandsüberweisungen.

Der nachfolgend geschilderte Betrugsfall beruht auf Tatsachen. Die Veröffentlichung soll gutgläubige Unternehmer und Manager davor bewahren, selbst auch zu Opfern derartiger Internet-Kriminalität zu werden.

1. Akt: Die Tat

Täter Nr. 1 ruft bei der Finanz-Chefin der amerikanischen Tochtergesellschaft einer deutschen Firmengruppe an. Er gibt sich als der deutsche Inhaber der Gruppe aus und fordert die amerikanische Controllerin auf, kurzfristig rund 350.000 US-Dollar in zwei Tranchen an ihr unbekannte Empfänger in Europa zu überweisen. Als Grund nennt er einen vorübergehenden Liquiditätsengpass bei einer anderen Tochterfirma, in deren Auftrag die Überweisungen

erfolgen sollen. Als vertrauensbildende Maßnahme bezieht sich der Täter auf einige Small-Talk-Details, die Wochen zuvor im E-Mail-Verkehr erwähnt worden waren. Offensichtlich war das US-Unternehmen erfolgreich gehackt worden. Der Anrufer schickt sodann eine E-Mail mit Nennung der beiden Bankverbindungen und der zu überweisenden Beträge. Und er kündigt die baldige Rückzahlung in die USA an. Als Absender wird eine gefälschte Mail-Adresse genutzt.

Als die vereinbarte Frist für die Rückzahlung ergebnislos verstrichen ist, wird die Finanz-Chefin allmählich von Zweifeln ergriffen. Sie beichtet das Geschehen der deutschen Geschäftsführung, die umgehend einen Krisenplan zur Schadensbegrenzung aufstellt.

2. Akt: Die Betrüger

Die Zahlungen erfolgen an eine kurz zuvor gegründete Briefkastenfirma in Kroatien und – erstaunlicherweise – an die Niederlassung einer bekannten Schmuckhandelskette in Wien.

Die dringende Rückfrage bei dem Niederlassungsleiter nach dem Verbleib von knapp 90.000 US-Dollar ergab folgendes: Täter Nr. 2 hatte sich kurz zuvor in dem Geschäft beraten lassen und sich für den „Erwerb“ einer Luxusuhr der genannten Preisklasse entschieden. Der Täter kündigte die Begleichung des Kaufpreises aus den USA an und vereinbarte, die Uhr nach Zahlungseingang abholen zu lassen. So geschah es: Die Niederlassung akzeptierte ohne Rückfrage die Zahlung eines ihr unbekannten amerikanischen Industrie-Unternehmens und händigte die Uhr aus an Täter Nr. 3, der sich als Abholer mit einem Personalausweis „legitimierte“. Die Besuche der Täter wurden mit Video-Kameras aufgezeichnet. Die Aufforderung des geschädigten deutschen Unternehmens, die Personaldaten und Videoaufnahmen der Täter zur Strafverfolgung herauszugeben, wurde von der Niederlassung aus Gründen des „Datenschutzes“ abgelehnt. Auch die Muttergesellschaft des Konzerns ließ eine Schadensersatzforderung wegen ungerechtfertigter Bereicherung anwaltlich zurückweisen. Angeblich ermitteln nun österreichische Behörden wegen des Verdachts der Geldwäsche.

Noch chaotischer präsentierten sich die Abläufe in Kroatien. Die dortige Bank, die zugunsten eines offensichtlich kriminellen, namentlich bekannten Kunden (Täter Nr. 4) immerhin etwa 260.000 US-Dollar ohne Rechtsgrund vereinnahmt hat, zeigte sich selbst nach dem Hinweis auf die bereits in den USA bestehende Strafanzeige völlig inkooperativ. Die Tochter einer österreichischen Bankgesellschaft lehnte jegliche Mithilfe bei der Sicherstellung der offenkundig betrügerisch erlangten Summe ab. Auch sonst gab es vor Ort keine nennenswerte Unterstützung. Die Handelsabteilung an der deutschen Botschaft in Zagreb konnte bzw. wollte lediglich mit einer Liste von in derartigen Betrugsfällen angeblich erfahrenen Anwaltssozietäten dienen. Das ausgewählte Büro forderte zunächst einen Vorschuss an, weitere Leistungen waren nicht erkennbar.

3. Akt: Versuch der Schadensbegrenzung

Auch das Engagement der deutschen Polizeibehörden hielt sich in engen Grenzen. So hat ein Sachbearbeiter des örtlichen Betrugsdezernats zunächst die Annahme eines Strafantrags verweigert, weil dafür die Behörden in den USA, Österreich und Kroatien zuständig seien. Erst nach Einschaltung des Polizeipräsidenten erklärte man sich zur formalen Amtshilfe bereit. Die Erwartung des geschädigten Unternehmens, durch Einbeziehung von BKA und Interpol unverzüglich zumindest das kroatische Bankkonto von Täter Nr. 4 beschlagnahmen zu lassen, erwies sich – vor dem Hintergrund der real existierenden Standards internationaler

Polizei-Kooperation – als blauäugig und unbegründet. Erst einige Zeit später kam die unbefriedigende Nachricht, dass die Summe ungehindert vom kroatischen Konto über eine Münchner Bank (sic!) ins Baltikum transferiert und dort unauffindbar versickert sei.

Für die geschädigte Firmengruppe löste das exotische Geschehen einen offenbar überfälligen Weckruf zur Etablierung zeitgemäßer Sicherungssysteme aus. Es führte aber auch zu der Erkenntnis, dass geschädigte Unternehmen in solchen Fällen mit von den Tätern bewusst herbeigeführten Grenzüberschreitungen kaum mit wirksamer Hilfe von Polizeibehörden, Staatsanwaltschaften, Rechtsanwälten und Banken rechnen können. Ein involvierter Anwalt resümierte einigermaßen rat- und sprachlos: „Ein Stück aus dem Tollhaus!“

4. Akt: Resümee

Als Glücksfall erwies sich die Tatsache, dass das geschädigte Unternehmen eine sogenannte „CEO Fraud“-Versicherung abgeschlossen hatte, so dass der wirtschaftliche Schaden letztendlich überschaubar war. Den meisten Firmenchefs ist weder das Risiko einer derartigen Bedrohung noch die Möglichkeit einer versicherungstechnischen Regulierung bekannt. Wer das Thema anspricht, bekommt häufig zu hören, dass man so „dämliches“ Verhalten im eigenen Zuständigkeitsbereich ausschließe. Die Mitarbeiter seien so konditioniert, dass sie nicht auf derartige Abzockereien hereinfielen. Unterschätzt wird dabei die Raffinesse solcher international agierenden Verbrecherbanden, die ihre Opfer durch die geschickte Vortäuschung falscher Personenidentitäten, durch den cleveren Aufbau von Vertrauen, durch künstlichen Zeitdruck und Psychoterror äußerst wirksam manipulieren.

Diese Form der globalen Internet-Kriminalität tritt seit 2013 immer häufiger auch im deutschen Wirtschaftsraum auf. Das Bundeskriminalamt hat in drei Jahren 250 Betrugsfälle erfasst. Die Dunkelziffer dürfte erheblich sein, weil vermutlich zahlreiche Opferfirmen einen Strafantrag wegen der vermeintlichen Blamage unterlassen. Dass er hier auch um existenzielle Größenordnungen gehen kann, zeigt der 2016 bei einem Automobilzulieferer entstandene Schaden von 40 Mio. Euro. Die weltweiten Schäden summieren sich einer FBI-Schätzung zufolge bereits auf 2,8 Mrd. Euro. Daraus resultiert als zentrale Handlungsempfehlung für alle verantwortlichen Führungskräfte, die eigenen Sicherungsstandards auch auf diese Bedrohung auszurichten und über angemessenen Versicherungsschutz nachzudenken.

Über den Autor: Der Unternehmer Dietrich W. Thielenhaus kommentiert aktuelle Entwicklungen in Politik und Wirtschaft.