CEO-Fraud: Wenn der „Chef“ zur Geldüberweisung auffordert

Reingelegt

Thomas Stasch

In den letzten ein bis zwei Jahren konnte man viel über den sogenannten CEO-Fraud lesen, auch Chef-Masche genannt. Auch beim Arbeitgeber des *iX*-Autors meldeten sich eines Tages solche Betrüger.

Ein CEO-Fraud ist, wie der Name sagt, ein Betrugsfall, bei dem der Geschäftsführer eines Unternehmens eine wichtige Rolle spielt. Oder genauer gesagt spielen eher der Name des Geschäftsführers und sein Führungsstil eine gewisse Rolle. Im Kern geht es darum, ein Unternehmen dazu zu verleiten, eine größere Geldsumme auf ein fremdes Konto zu überweisen.

Aber fangen wir einfach einmal vorne an: In dem Unternehmen, für das ich tätig bin – ein kommunaler IT-Dienstleister beziehungsweise dessen CERT –, kam es zu einem Fall von CEO-Fraud mit dem Ziel, uns um 455 000 Euro zu erleichtern.

Anbahnung per E-Mail

Eines Tages erhielt ich einen Anruf von unserem obersten Finanzleiter: „Ich glaube, ich habe da so einen Betrugsfall, von dem du schon einmal erzählt hast.“ Um genauer zu sein: Er hatte die erste Anbahnungs-E-Mail erhalten. Der Kollege hatte eine Mail mit dem Geschäftsführer als Absender im Posteingang, in der dieser vorsichtig nachfragte, ob der Kollege den ganzen Tag verfügbar sei. Es ging darum, eine streng vertrauliche Sache vorzubereiten.

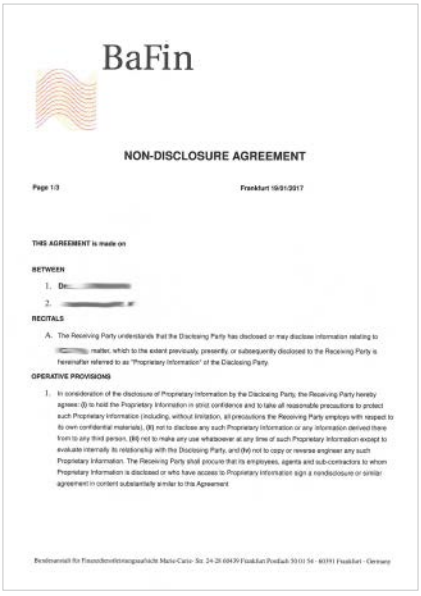
Der Blick auf die Absenderadresse verriet allerdings schon, dass die Mail nicht vom Geschäftsführer gekommen war, sondern man dies nur vortäuschen wollte. Sprich: Der angezeigte Name war zwar der des Geschäftsführers, dahinter verbarg sich aber eine Adresse, die nicht zum Unternehmen gehörte. Die gleiche Methode sehen wir übrigens auch in der aktuellen Emotet-Welle. Hier verbergen sich ebenfalls andere Mailadressen hinter den angezeigten Namen.

Damit war für uns die Sache klar. Eine kurze Abstimmung innerhalb des CERT, Rücksprache mit dem Finanzleiter und schon konnte der Spaß losgehen. Wir hatten beschlossen, auf das Spiel einzugehen, um den Verlauf und die Vorgehensweise der Betrüger zu studieren. Gleichzeitig wurde das Landeskriminalamt informiert und Strafanzeige wegen des Verdachts auf Betrugsanbahnung erstattet.

Entsprechend positiv antwortete der Finanzleiter auf die Mail: Selbstverständlich stünde er zur Verfügung. Diese Antwort wurde mit einem Tracking-Pixel versehen, um vielleicht ein paar Anhaltspunkte zu erhalten. Schnell entwickelte sich ein Dialog zwischen „Geschäftsführer“ und „Finanzleiter“, besser gesagt zwischen dem Betrüger und unserem CERT. Die Tracking-Pixel zeigten, dass die andere Seite mit Verschleierungsmethoden arbeitete, da die E-Mails abwechselnd aus dem UK, aus Serbien und aus Deutschland abgerufen wurden.

Schneller akquirieren als die Konkurrenz

Der Betrugsversuch gaukelte eine streng vertraulich zu handhabende Firmenübernahme vor, die eingeleitet werden musste,



BaFin

NON-DISCLOSURE AGREEMENT

Page 1/3 Frankfurt 19/01/2017

THIS AGREEMENT is made on

BETWEEN

1. De...
2. ...

RECITALS

A. The Receiving Party understands that the Disclosing Party has disclosed or may disclose information relating to ... matter, which to the extent previously, presently, or subsequently disclosed to the Receiving Party is hereinafter referred to as "Proprietary Information" of the Disclosing Party.

OPERATIVE PROVISIONS

1. In consideration of the disclosure of Proprietary Information by the Disclosing Party, the Receiving Party hereby agrees: (i) to hold the Proprietary Information in strict confidence and to take all reasonable precautions to protect such Proprietary Information (including, without limitation, all precautions the Receiving Party employs with respect to its own confidential materials), (ii) not to disclose any such Proprietary Information or any information derived there from to any third person, (iii) not to make any use whatsoever at any time of such Proprietary Information except to evaluate internally its relationship with the Disclosing Party, and (iv) not to copy or reverse engineer any such Proprietary Information. The Receiving Party shall procure that its employees, agents and sub-contractors to whom Proprietary Information is disclosed or who have access to Proprietary Information sign a nondisclosure or similar agreement in content substantially similar to this Agreement

Eine Verschwiegenheitserklärung sollte Seriosität vortäuschen und den zuständigen Finanzleiter beschäftigen (Abb. 1).

BaFin

Request of payment

Dear Mr. ..., please find attached the bank details and the amount to proceed to the wire transfer urgent express forthe first down payment regarding this acquisition.

File Reference: 2655-2926/PL

Date of the request for payment: ...

The amount requested is of 455.000.00 €

Amount: 455.000.00€

Beneficiary: ...

Bank: ...

IBAN: ...

BIC/SWIFT CODE: ...

Please send me a copy of the "priority swift transfer" as soon as possible, so that I can inform the Lawyers on the counterpart in real time and attach it to the file.

Über die Kontodaten der Betrüger freuten sich insbesondere die Ermittler des LKA (Abb. 2).

bevor Presse und Konkurrenz davon Kenntnis erlangen konnten. Sehr schön war zu erkennen, wie professionell versucht wurde, den Gedanken auf diese Übernahme und die Vertraulichkeit fokussiert zu halten und den Finanzleiter vom eigentlichen Ziel abzulenken.

So musste beispielsweise eine Vertraulichkeitserklärung unterzeichnet werden (Abbildung 1). Das führte innerhalb des CERT dazu, dass die zugesandten PDF-Dokumente detailliert auf mögliche Schadcodes geprüft wurden, bevor man eine „unterschriebene" Fassung wieder zurückschickte. Parallel dazu bestand durchgehend Kontakt zum LKA. Laut Auskunft der LKA-Ermittler sind solche CEO-Frauds leider oft tatsächlich erfolgreich und die Schadenshöhen immens.

In die Kommunikation zwischen „Finanzleiter" und „Geschäftsführer" stieg plötzlich noch ein „Anwaltsbüro" ein – hinter dem sich natürlich ebenfalls die betrügerische Seite verbarg: Mitten in die betriebliche Hektik fiel ein Anruf unseres Finanzchefs mit den Worten: „Ich habe eben einen Anruf von dem angeblichen Anwalt bekommen." Eine neue Phase des betrügerischen Vorgehens war eingeläutet. Die Rufnummer des Finanzchefs wurde nun auf das CERT umgeleitet und tatsächlich: Abends kam es zu einer erneuten Kontaktaufnahme.

Realität versus Fernsehkrimi

Insgesamt sieben Minuten dauerte das erste Telefonat des angeblichen Anwaltsbüros und es fand auf Englisch statt. Darin wurde ein Folgetermin für eine kurze Telefonkonferenz für den nächsten Tag um 9 Uhr mitteleuropäischer Zeit anberaumt. Die sofortige Rücksprache mit dem LKA zeigte, dass sich Fangschaltungen beim Tatort in der ARD deutlich schneller umsetzen lassen als in der Realität.

Die nächsten vier bis fünf Telefonate führten dann langsam in Richtung des eigentlichen Verbrechens. Die Betrüger loteten vorsichtig aus, welche Höchstsumme durch den kaufmännischen Leiter freigegeben werden kann. In unserem Fall gaukelten wir vor, dass der Finanzchef alleine bis 500 000 Euro freizeichnen könne. Darüber hinaus lockten wir damit, dass nach dem Wochenende der zweite Kollege wieder da wäre, mit dem man zusammen über maximal 2,5 Mio. verfügen könne.

Zwischendurch fragte ich mich immer wieder: „Wieso merkt der Betrüger nicht, dass ich ihn hinhalte und die ganze Zeit an der Nase herumführe?" Irgendwann wurde mir klar, dass er so stark auf sein Ziel fokussiert war, Geld zu erbeuten, dass ihm wahrscheinlich gar nicht auffiel, welche ungewöhnlichen Fragen ich ihm zwischendurch immer wieder stellte, um der Polizei mehr Ermittlungsansätze zu liefern.

An einem Freitagmittag war es dann so weit. Das Finale hatte begonnen. Wir erhielten die Aufforderung, den Betrag von 455 000 Euro zu überweisen – also innerhalb der angeblichen Freizeichnungsgrenze. Ebenso wurde eine IBAN übermittelt, auf die das Geld zu transferieren war (Abbildung 2). Das war insbesondere für das LKA ein Ermittlungserfolg, da das Bankkonto im europäischen Ausland lag. Mit meiner Versicherung, dass wir überwiesen hätten, war dann der Fall abgeschlossen – dachten wir.

Faktoren für das Gelingen eines Betrugs

Montags ging ein neuer Anruf ein: Nachdem nun die erste Phase erfolgreich abgeschlossen sei, müsse man sich an die Phase zwei machen. Der Betrüger hatte offensichtlich wegen der angeblichen Möglichkeit angebissen, weitere 2,5 Mio. zu ergaunern. Auf Anraten des LKA brachen wir an dieser Stelle ab.

Insgesamt war dieser Fall hochinteressant. Er zeigte uns, wie perfekt solche Vorgehen geplant und umgesetzt werden. Leider fallen immer wieder Firmen auf eine derartige Masche herein. Woran mag das liegen? Es ist sicherlich ein Zusammenspiel verschiedener Faktoren, das es möglich macht, mit einem CEO-Fraud große Geldsummen zu erbeuten.

Wirkungsvolle Gegenmaßnahmen sind beispielsweise ein von Respekt und Offenheit gekennzeichneter kooperativer Führungsstil, der einfache Rücksprachen in einem Unternehmen ermöglicht. Ein Finanzchef, der Angst vor seinem Geschäftsführer hat, wird viel eher in Bedrängnis kommen. Denn er will nichts Falsches machen und wird dem Druck nachgeben, den die Betrüger so kunstvoll und mit genau dieser Absicht aufbauen.

Eine weitere wirkungsvolle Gegenmaßnahme ist die Schulung und Sensibilisierung aller Mitarbeiter. Wenn – wie in unserem Fall – der Leiter des Finanzbereiches sofort erkennt, dass die erste Mail gar nicht von seinem Vorgesetzten kommt, läuft der Angriff direkt ins Leere. Unabhängig davon empfiehlt es sich immer, die zuständige Polizei oder besser noch eine entsprechende Cyber-Crime-Unit zu kontaktieren und Strafanzeige zu erstatten.

Das BKA hat eine Broschüre mit Tipps zum Thema CEO-Fraud veröffentlicht (Abb. 3).

Das BKA hat eine Broschüre verfasst (Abbildung 3, über ix.de/ix1906078 zu finden), die weitere Vorsichtsmaßnahmen nennt. So rät die Behörde etwa, zurückhaltend zu sein mit dem Veröffentlichen von Informationen über das Unternehmen. Außerdem empfiehlt sie das Etablieren klarer Abwesenheitsvertretungsregelungen nebst internen Kontrollmechanismen.

Abschließend sei auch noch einmal ausdrücklich darauf hingewiesen, dass ein angebliches Eingehen auf eine solche Masche nur in enger Abstimmung mit den Ermittlungsbehörden erfolgen sollte. Hinter diesen Angriffen stecken Profis, mit denen nicht zu spaßen ist. (ur@ix.de)

Quellen

Die im Text erwähnte BKA-Broschüre ist über den Link ix.de/ix1906078 zu finden.

Thomas Stasch

ist Leiter des civitec-CERT beim kommunalen IT-Dienstleister civitec in Siegburg und Dozent für Informationssicherheit an der Wilhelm-Büchner-Hochschule Darmstadt.