ComplianceBusiness
Ausgabe 1 // März 2017

Die Kehrseite der Transparenz

Im Blickpunkt: CEO-Fraud und wie sich Unternehmen davor schützen können

Von Bodo Meseke und Burim Ferati

Einleitung

In Anbetracht der aktuellen Ereignisse in Politik und Wirtschaft wie etwa Panama Papers oder VW-Abgasskandal ist eine zunehmende Forderung nach erhöhter Transparenz feststellbar. Gerade Unternehmen versuchen, diesem Ruf mehr und mehr gerecht zu werden – sei es durch zum Teil sehr umfangreiche Geschäfts- und Wirtschaftsberichte, detaillierte Internetauftritte oder Werbebroschüren. Eine ähnliche Entwicklung ist auf Unternehmens- wie auch auf Mitarbeiterebene in Verbindung mit Social-Media-Auftritten zu beobachten. Diese Offenlegungskultur und Transparenz erfreut auf der einen Seite die Stakeholder, lockt auf der anderen Seite aber auch betrügerische Banden, die diese Transparenz zum Teil gnadenlos ausnutzen.

Die Identität und Legitimität des „Chefs“ muss vor einer Auszahlung mit gezielten Kontrollprozessen geprüft werden.

Das Bundeskriminalamt (BKA) warnte bereits zum letzten Jahreswechsel und zuletzt vergangenen Sommer eindringlich vor dem sogenannten CEO-Fraud, der auch als „Chef-Masche", „Fake President" oder „Enkeltrick 4.0" bezeichnet wird. So berichtet Holger Kriegeskorte, Leiter des Sachgebiets für Wirtschaftskriminalität des BKA, dass man seit dem Jahr 2013 etwa 250 Betrugsfälle dokumentiert habe. Insgesamt seien 68 Delikte erfolgreich verlaufen, wodurch ein Gesamtschaden von mehr als 110 Millionen Euro für die betroffenen Unternehmen entstanden sei. Die Dunkelziffer dürfte jedoch weitaus höher liegen, weil viele Unternehmen einen Reputationsverlust vermeiden wollen oder ihnen der Vorfall zu peinlich ist, um ihn bei der Polizei zu melden.

CEO-Fraud-Geschädigte finden sich in allen Gesellschaftsformen und -größen – vom Mittelständler bis zum DAX-Konzern, egal ob im Bankensektor, im produzierenden Gewerbe oder im Dienstleistungssektor. Neben zahlreichen anderen Unternehmen, die dem CEO-Fraud zum Opfer gefallen sind, hat zuletzt auch der Automobilzulieferer Leoni AG bekanntgegeben, dass man dieser Betrugsform zum Opfer gefallen sei und einen Schaden von circa 40 Millionen Euro erlitten habe.

Enkeltrick 4.0 – oder: Wie funktioniert der CEO-Fraud?

Oft ergeben sich im Rahmen der Aufarbeitung die immer gleichen Fragen: Wie konnte es überhaupt dazu kommen? Wie funktioniert der CEO-Fraud? Allen voran aber: „Wieso haben unsere internen Prozesse versagt?" und: „Wie hätte es verhindert werden können?"

Die Täter nutzen die angesprochene Offenheit und Transparenz der Unternehmen und der Mitarbeiter in Geschäfts- und Wirtschaftsberichten, Internetauftritten oder in Social-Media-Plattformen aus, um sich Insiderwissen zu verschaffen und gezielt Mitarbeiter im Unternehmen anzusprechen. Die Täter werten alle verfügbaren Informationen aus und fügen sie zu einem plausiblen Business-Case zusammen, um die Unternehmen möglichst gezielt anzugreifen. Dabei helfen ihnen beispielsweise Wirtschaftsberichte, um geplante Transaktionen zu identifizieren. Businessplattformen wie etwa XING oder LinkedIn werden genutzt, um die aufgrund ihrer Funktion „richtigen" Mitarbeiter im Unternehmen festzustellen.

Sobald diese Informationen gesammelt sind, geht ein Anruf oder eine E-Mail vom „Chef" persönlich bei der Zielperson aus der Buchhaltung ein und drängt zu Eile und absoluter Diskretion. Es müsse dringend eine große Summe Geld nach China, Hongkong oder nach Osteuropa überwiesen werden. Die Transaktion habe oberste Priorität für die Geschäftsbeziehungen des gesamten Unternehmens. Meistens handelt es sich dabei um Patentrechte, Firmenanteile, Immobilien oder Maschinen, die angeschafft werden sollen. Eine fadenscheinige Dokumentation der Kommunikation zur Absicherung der handelnden Personen wird dabei per E-Mail vorgenommen.

Die Täter nutzen dazu Instrumente wie etwa nahezu identische E-Mail-Adressen, die dem Look and Feel (Signatur, Logo, Schreibstil etc.) der echten Unternehmenskommunikation entsprechen, oder bereiten mit vorhergehenden Anrufen den Angriff vor, um sogar eine Dokumentation per E-Mail noch abzuwenden. So kam es in einem Fall vor, dass der „Chef" einer Mitarbeiterin aus der Buchhaltung mehrere Wochen vor dem Angriff telefonisch zum Dienstjubiläum gratulierte, um auf diese Weise die Mitarbeiterin mit seiner Stimme vertraut zu machen, bevor dann der Anruf bezüglich der geforderten Überweisung auf ein Bankkonto des Anrufers kam. Überwältigt vom Anruf des „Chefs", dem dahinterliegenden Zeitdruck und mit der naiven Gewissheit, es schaue „noch ein Zweiter drüber", führt die Mitarbeiterin oder der Mitarbeiter den Auftrag aus. Die gezahlten Geldbeträge gehen in den unzähligen Positionen eines Zahllaufs unter. Sobald das Geld überwiesen ist, geht alles ganz schnell. Die zuvor unter falschem Namen im Ausland eingerichteten Bankkonten werden sofort leergeräumt, und bei den verwendeten Mobilfunknummern handelt es sich in der Regel um Prepaid-Nummern, die nicht nachzuverfolgen sind. Die Chance, das Geld wiederzubekommen, tendiert gen null.

Angesichts derartiger Vorkommnisse wird sicherlich die Frage aufkommen, ob man zum eigenen Schutz die Transparenz einschränken sollte. Ob dies letztlich das Allheilmittel wäre, lässt sich aus heutiger Sicht nicht beantworten. Vieles spricht dagegen – nicht zuletzt gesetzliche Anforderungen. Ein effektiver Schutz davor, Opfer einer solchen Betrugsmasche zu werden, liegt vielmehr in der Sensibilisierung potentiell gefährdeter Mitar-

beiter oder auch in der Schaffung eindeutiger und verlässlicher Richtlinien und Strukturen. So kann ein sensibilisierter Mitarbeiter einen solchen Angriff meist sehr schnell ins Leere laufen lassen, indem er die ungewöhnliche Zahlungsaufforderung durch einen Anruf beim „Auftraggeber" verifiziert.

Gegenwärtig erscheinen eine Sensibilisierung der Mitarbeiter beispielsweise durch Schulungen und eine Überprüfung der internen Kontrollen als weitaus effizientere Lösungen im Vergleich zur Einschränkung der Transparenz.

Informieren und kommunizieren

Viele der genannten 250 Betrugsfälle konnten primär durch aufmerksame und sensibilisierte Mitarbeiter verhindert werden. Hierzu bedarf es einer maßvollen und adressatengerechten Kommunikation. Schulungen und Trainings sind dabei ein wirkungsvolles Instrument. Besonders wichtig sind Lehr- und Lernkonzepte, die gezielt digitale Informations- und Kommunikationsmedien in einem für jeden zugänglichen Medienmix nutzen.

Interne Kontrollmechanismen ...

Eine derart einfache Betrugsform wie der CEO-Fraud zeigt deutlich auf, wo die gravierendsten Schwachstellen in einem Unternehmen zu liegen scheinen: in nicht ausreichend wirksam implementierten Kontroll- und Freigabeprozessen (etwa Vieraugenprinzip), unverschlüsseltem E-Mail-Verkehr und der zum Teil immer noch weitverbreiteten Meinung, so etwas könne im eigenen Unternehmen nicht passieren.

Dabei lässt sich mit einfachen Mitteln meist sehr viel bewirken, beispielsweise durch die Neujustierung der internen Warnsysteme, die Hinweise abgeben, bevor der Geldtransfer ausgeführt wird, oder durch das Schaffen klarer Strukturen und Prozesse für derartige Ad-hoc-Transfers (etwa für Zahlungen an unbekannte Konten oder Stammdaten).

Es hat sich gezeigt, dass präventive Maßnahmen wie etwa die beschriebene Sensibilisierung der Mitarbeiter und die Schaffung klarer Strukturen und Richtlinien insbesondere im Zusammenhang mit CEO-Fraud weitaus effizienter sind als die nachgelagerte IT-Forensik. Die Tat erfolgt binnen einer kurzen Zeitspanne, so dass der Schaden bereits entstanden ist, bevor die IT-Forensiker den Fall aufarbeiten können.

... und Aufgaben des Vorstands und Aufsichtsrats

Angesichts der zahlreichen Fälle sollten sowohl beim Vorstand als auch beim Aufsichtsrat international tätiger Unternehmen die Alarmglocken läuten. Diese Betrugsform ist bereits seit 2013 bekannt, so dass Vorstand und Aufsichtsrat im Rahmen ihrer Aufsichtspflicht und Kontrollfunktion die Pflicht haben, regulatorische und organisatorische Vorkehrungen zu treffen, um derartige Risiken zu minimieren. Schließlich schützt Unwissenheit nicht vor Strafe.

Bodo Meseke,
Partner, Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft, Fraud Investigation & Dispute Services, Frankfurt am Main/Eschborn

bodo.meseke@de.ey.com
www.de.ey.com

Burim Ferati,
Manager, Ernst & Young GmbH Wirtschaftsprüfungsgesellschaft, Fraud Investigation & Dispute Services, Frankfurt am Main/Eschborn

burim.ferati@de.ey.com
www.de.ey.com