CB-EDITORIAL

Cybercrime Reloaded – vom Opfer zum Täter?

Chefbetrug, CEO-Fraud – die Masche der modernen Enkeltrick-Betrüger ist heute faktisch ein alter Hut. Das tut dem Phänomen aber keinen Abbruch. Weiterhin schädigen Betrüger massiv v. a. mittelständische Unternehmen. Betrüger, die mit technisch immer raffinierteren Methoden Mitarbeiter täuschen, um an Geld zu kommen.

Lassen wir die technische Raffinesse einmal beiseite, so prägt solide vorbereitetes „Social Engineering" den modus operandi der Straftäter: Sie setzen das Wissen um, dass Mitarbeiter bestimmte Dinge gern hören, andere Situationen hingegen unbedingt vermeiden wollen. Dass vertrauensvolle Interaktion mit der ersten Führungsebene als ebenso selten wie erstrebenswert gilt. Dass in vielen Unternehmen die Angst, das Falsche zu tun und sich damit Aufstiegschancen zu ruinieren, vorherrschend ist.

Betrugsopfer, gerade im wirtschaftsstrafrechtlichen Kontext, wird man besonders leicht dann, wenn entweder Gier oder aber Angst das eigene Handeln beeinflusst. Sämtliche mühsam antrainierten Vorsichtsmaßnahmen sind gerade dann vergessen, wenn das letzte zum Thema passende web based trainig zwischen den verschiedenen Datenschutzgrundverordnungs-Erklärvideos und Code of Conduct-Exzellenzinitiativen förmlich untergegangen ist.

Für Unternehmen bedeutet diese Entwicklung eines: Ein Perspektivwechsel ist nötig! Zwar ist es richtig, dass im Falle von Cybercrime, etwa beim Chefbetrug, das Unternehmen noch immer Opfer ist, nicht Täter. Jedoch spielt hier die Zeit gegen die Belange der Geschäftsleitung und – schlimmstenfalls – auch der durch Betrüger manipulierten Mitarbeiter.

Das hat folgenden Grund: Je bekannter die Methodik der Straftäter ist, weil etwa Informationsquellen zum Thema leicht zugänglich sind, desto näher liegt es, bei einer „Opferwerdung" des Unternehmens verstärkt an eine Pflichtverletzung des Managements zu denken. Kurz: Wer seine Compliance-Struktur nicht regelmäßig an das reale Bedrohungsszenario anpasst, allgemein bekannte Risiken und deren Auswirkungen auf das eigene Unternehmen nicht angemessen oft analysiert, diese Pflichten nicht wirksam delegiert – das von ihm geführte Unternehmen also nur unzureichend gegen die vielfältigen Bedrohungslagen im Bereich Cybercrime schützt – verletzt seine Compliance-Pflichten, und macht sich dadurch angreif- und haftbar.

Konkrete Folge, etwa im Follow-up eines größeren Falles von CEO-Fraud: Der Aufsichtsrat wäre verpflichtet, eine Schadenersatzpflicht der Geschäftsleitung zu prüfen, den Vorgang dazu untersuchen zu lassen und ggf. Organhaftungsverfahren voranzutreiben. Prognose nach vielfachen themenbezogenen Ermittlungsverfahren zahlreicher Staatsanwaltschaften und verschiedener Diskussionen mit Strafverfolgern zum Thema Pflichtwidrigkeit und (auch strafrechtlich) relevanter Schaden: Nach einer Schadensmeldung an die D&O- sowie auch der Vertrauensschadenversicherung wird der Streit, ob die erlebte Opfersituation vorhersehbar und vermeidbar gewesen wäre, sehr intensiv geführt werden. Führungskräfte müssten sich mehr denn je auf verschiedenen rechtlichen Ebenen rechtfertigen, weshalb sie in einem bekanntermaßen gefährdeten Umfeld genügende Schutzmaßnahmen mit Blick auf das von ihnen zu betreuende Unternehmensvermögen unterlassen haben.

Ein Perspektivwechsel ist nötig! Die Zeit spielt gegen die Belange der Geschäftsleitung.

Damit könnte auch das Unternehmen selbst nach einer sog. Anordnung der Nebenbeteiligung in den Fokus rücken: Zwar ist es durch die eigentliche Betrugshandlung buchstäblich „gestraft genug". Allerdings könnte bspw. eine Staatsanwaltschaft untersuchen, ob die an das Management gerichtete Pflichtenmahnung: „Du sollst geeignete Maßnahmen implementieren, um greifbaren Gefahren für das Vermögen des Unternehmens, das Du führst, wirksam zu begegnen!" eingehalten wurde oder nicht. Mit Blick auf das ordnungswidrigkeitenrechtliche Regime aus Verbandsgeldbuße und Verletzung der Aufsichtspflicht sowie Untreue durch Unterlassen als Anknüpfungstat eine rechtlich interessante, praktisch durchaus kostspielige Entwicklung.

Zu denken wäre schließlich – im Falle regulierter Industrien – auch an durch die jeweils zuständige Aufsichtsbehörde veranlasste Konsequenzen personeller Natur: Ob deren Feststellungen zu einem mangelhaften Internen Kontrollsystem zur Vermeidung sonstiger Straftaten zu Veränderungen innerhalb der Compliance-Funktion oder der zweiten Führungsebene führen, interessiert in der Praxis kaum. Zentrale Frage wird etwa bei sich anschließenden Haupt-, Gesellschafter- oder Vertreterversammlungen sein, weshalb es die Geschäftsleitung so weit hat kommen lassen.

AUTOR

Jörg Bielefeld *ist Rechtsanwalt und Partner bei BEITEN BURKHARDT in Frankfurt und München. Er leitet den Bereich Wirtschaftsstrafrecht und Compliance.*