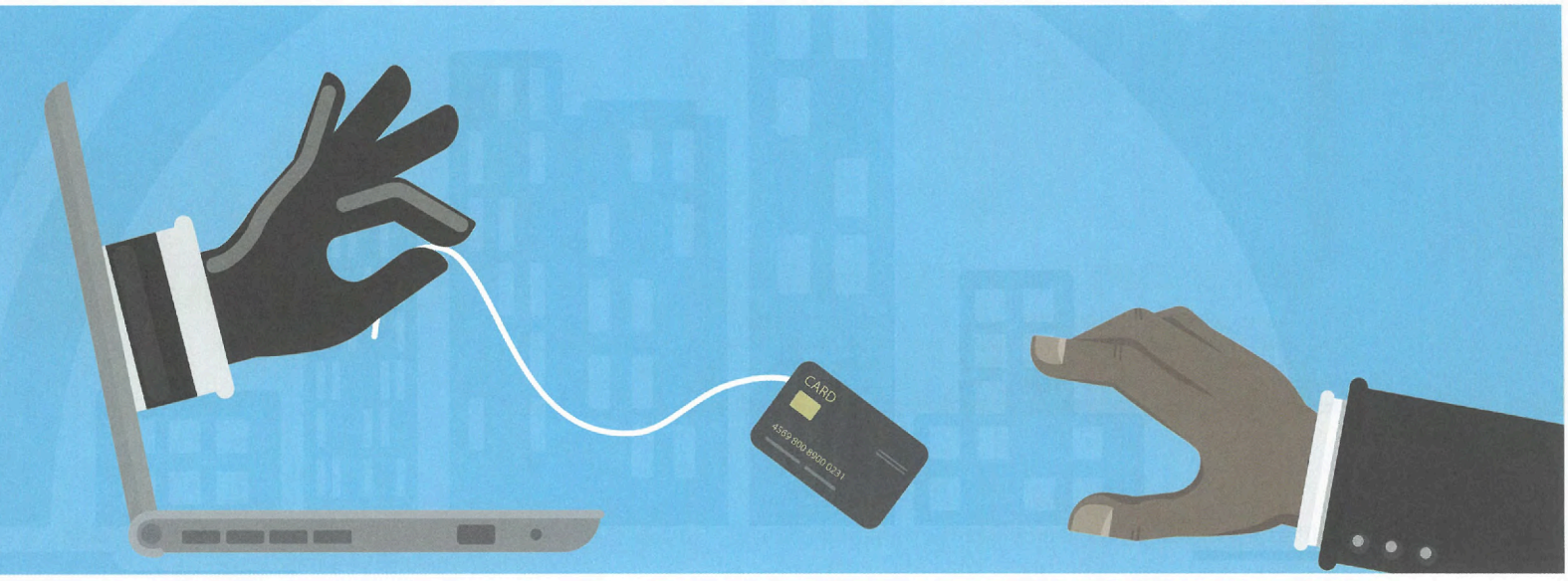

Haftung & Prävention: Aktuelle Antworten zum „Fake President Fraud“

Eine rezente Entscheidung des OGH (8 ObA 109/20t) befasst sich mit der Haftung eines Geschäftsführers für den finanziellen Schaden, der durch einen „Fake President Fraud“ verursacht wurde. Der folgende Artikel erläutert vor dem Hintergrund der Entscheidung, welche Präventionsmaßnahmen Unternehmen gegen diese trickreiche Betrugsmethode ergreifen können.

Von Elias Schönborn und Julian Spadinger

Allgemeines

Beim Fake President Fraud (im Folgenden kurz „FPF“) handelt es sich um eine Betrugsmethode, bei der Mitarbeiter eines Unternehmens gezielt manipuliert werden, um letztlich große Beträge auf andere (oftmals ausländische) Konten zu überweisen. Typischerweise wird dabei dem Mitarbeiter glaubhaft gemacht, dass die Transaktion von einer Autoritätsperson (zB der Geschäftsführung, einer Aufsichtsbehörde usw) genehmigt oder in Auftrag gegeben wurde. Um Zweifel des Mitarbeiters möglichst auszuräumen, bedienen sich die Betrüger bei der Kontaktaufnahme bestimmter Daten und Informationen, die bereits im Vorfeld etwa durch gehackte bzw sehr ähnlich wirkende E-Mail-Accounts oder umfangreiche Recherchen über das Unternehmen eruiert wurden. Dadurch täuschen die Täter Authentizität vor und bauen ein künstliches Vertrauensverhältnis auf.

Die Methode des FPF ist darauf ausgelegt, die internen Kontrollmechanismen eines Unternehmens auszuhebeln. Das zu dem Mitarbeiter aufgebaute Vertrauensverhältnis soll diesen letztlich dazu bringen, eine Überweisung auch unter Missachtung bestehender Überprüfungsmechanismen durchzuführen. Daher reicht zur Verhinderung von FPF ein herkömmliches Internes Kontrollsystem (IKS) meist nicht aus. Vielmehr bedarf es zusätzlicher Präventionsmaßnahmen, die dem besonderen Charakter dieser Betrugsmethode gerecht werden.

Judikatur und Haftungsfragen

Der OGH hatte unlängst in seiner Entscheidung 8 ObA 109/20t die Haftung eines Geschäftsführers gegenüber einer von einem FPF betroffenen GmbH, die dadurch über 50 Millionen Euro verlor, zu beurteilen. Die letztlich haftungsverneinende Entscheidung gibt →

Aufschluss darüber, wie weit Präventionsmaßnahmen in Bezug auf derartige Betrugsformen reichen müssen, um sich noch im Rahmen der ordnungsgemäßen Geschäftsführung zu bewegen. Aufgrund der Tatsache, dass der FPF gerade das Ziel verfolgt, bestehende Kontrolleinrichtungen zu umgehen und die Betrugsmethode gleichzeitig – außerhalb von Fachkreisen – in Österreich bislang nicht hinreichend bekannt ist, enthält die Entscheidung des OGH einige bemerkenswerte Klarstellungen. Bei der Haftungsfrage, die sich Geschäftsführer regelmäßig stellen, ist jedenfalls Vorsicht geboten, da der FPF in den letzten Jahren an Bekanntheit gewonnen hat und die vorliegende Entscheidung – die auch medial aufgearbeitet wurde – noch weiteren Anlass zu Nachschärfungen geben dürfte. Compliance-Beauftragten, Mitarbeitern der Internen Revision und (ressortzuständigen) Geschäftsführern ist daher zu raten, bereits bestehende IKS in ihrem Compliance-Management-System mit Blick auf diese Betrugsmethode im Bedarfsfall zu adaptieren. Im Folgenden werden daher Maßnahmen dargestellt, welche die Besonderheiten des FPF berücksichtigen.

Mögliche Präventionsmaßnahmen

Präventive Maßnahmen können an unterschiedlichen Stadien des Betrugsprozesses ansetzen. Durch die Etablierung eines wirksamen IT-Systems kann bereits die erforderliche Informationsbeschaffung der Betrüger erschwert werden. Kommt es dennoch zur Kontaktaufnahme zu einem Mitarbeiter, wird sich dieser am ehesten dann richtig verhalten, wenn im Vorfeld eine Sensibilisierung für das Thema im Unternehmen stattgefunden hat. Schließlich ist auch die Einrichtung eines verbindlichen, transparenten und effektiven Zahlungsfreigabesystems essenziell, um rechtswidrige Überweisungen vom Firmenkonto zu verhindern.

Abwehr 1: Sicheres IT-System

Wie eingangs dargestellt, geht einem erfolgreichen FPF-Angriff meist eine umfassende Informationsbeschaffung der Täter voraus. Dabei werden neben frei zugänglichen Daten auch vertrauliche Informationen durch gezielte Hacking-Angriffe gesammelt. Eine funktionierende IT-Organisation, die von den Verantwortlichen des Unternehmens im Rahmen ihrer Sorgfaltspflichten einzurichten ist, kann potenzielle Angriffe daher zumindest erschweren.

Abwehr 2: Sensibilisierung und Speak-Up-Kultur

Die Betrugsform des FPF setzt an der psychologischen Manipulierbarkeit von Mitarbeitern an. Durch Betonung der besonderen Vertraulichkeit und gebotenen Geheimhaltung des Zahlungsvorgangs und unter Ausnutzung des Pflichtbewusstseins vor einer Autoritätsperson wird der Mitarbeiter selbst bei bestehenden Zweifeln davon abgehalten, Arbeitskollegen und Vorgesetzte zu informieren bzw zu konsultieren. Präventionsmaßnahmen müssen daher das Ziel haben, eine solche Isolation und Manipulation des Mitarbeiters bereits im Vorfeld zu verhindern. Dies kann etwa mit Schulungsmaßnahmen und einer Arbeitspraxis im Unternehmen erreicht werden, die den Informationsaustausch fördert und Mitarbeiter geradezu anregt, bei aufkommenden Zweifeln das Gespräch mit einem Vorgesetzten zu suchen.

Die Autoren

Dr. Elias Schönborn ist Rechtsanwalt bei DORDA und auf Criminal Compliance und Wirtschaftsstrafrecht spezialisiert.

Julian Spadinger ist Trainee in der Arbeitsgruppe Dispute Resolution und Wirtschaftsstrafrecht bei DORDA.

Zusätzlich ist es zweckmäßig, ein allgemeines Gefahrenbewusstsein für derartige Betrugsmethoden zu schaffen, wobei auch von der abschreckenden Wirkung durch den Hinweis auf straf- und zivilrechtliche Folgen (inklusive arbeitsrechtliche Konsequenzen) Gebrauch gemacht werden kann.

Abwehr 3: Verbindliches Nachschlagewerk

Sollte es dennoch zu einer Isolation eines Mitarbeiters kommen, ist es von Vorteil, wenn das Zahlungsfreigabesystem des Unternehmens (als Teil eines funktionierenden IKS) bereits im Vorfeld schriftlich festgehalten wurde. Dabei ist es wichtig, dass den verschriftlichten Vorgaben eine hohe Verbindlichkeit zukommt und auch in der alltäglichen Praxis ausnahmslos keine davon abweichenden Zahlungsprozesse stattfinden.

Abwehr 4: Zahlungsfreigaben nach dem Vier-Augen-Prinzip

Inhaltlich hat sich in der unternehmerischen Praxis im Zusammenhang mit einem Zahlungsfreigabesystem das „Vier-Augen-Prinzip" bewährt. Zahlungsvorgänge erfordern demnach die Autorisierung zweier voneinander unabhängiger Mitarbeiter. Ein „Social Engineering"-Angriff bei einem FPF bezweckt es allerdings, gerade derartige Systeme zu umgehen – daher muss neben der Verpflichtung per se auch die effektive Einhaltung sichergestellt werden. In diesem Zusammenhang ist einmal mehr auf die zuletzt ergangene OGH-Entscheidung einzugehen. Nach den getroffenen Feststellungen war im betroffenen Unternehmen ein „Vier-Augen-Prinzip" vorgesehen, dessen Einhaltung durch zwei voneinander getrennt aufzubewahrende PIN-Codes sichergestellt werden sollte. Dennoch gelang es einer Mitarbeiterin (Gruppenleiterin der Finanzbuchhaltung), dieses System zu überwinden, da sämtliche PIN-Codes entgegen dem Gebot der räumlich getrennten Aufbewahrung bei ihr in einer Mappe gesammelt waren und sie die Zahlungen so allein durchführen konnte. Der OGH verneint im konkreten Fall zwar die Verpflichtung zur weitergehenden Kontrolle der Zahlungsprozesse – zu beachten ist aber, dass sich diese Entscheidung auf einen Geschäftsführer bezieht, der für die Finanzbuchhaltung und damit die Zahlungsprozesse gar nicht ressortzuständig war.

Unabhängig von den dargestellten Haftungsfragen interessiert im gegenständlichen Zusammenhang aber, auf welche Weise einem Zahlungsfreigabesystem wie dem Vier-Augen-Prinzip tatsächlich zum Durchbruch verholfen werden kann. Grundsätzlich stellt ein Code-System mit unterschiedlichen Aufbewahrungsorten hier durchaus ein probates Mittel dar, allerdings muss sichergestellt sein, dass diese physische Trennung auch wirklich besteht, um zu vermeiden, dass Mitarbeiter aufgrund des Zugangs zu mehreren PIN-Codes unkontrolliert Überweisungen vornehmen können. Zu überlegen wäre auch, ob ein Berechtigungsmanagement im Rahmen der IT-Organisation, das zB mittels biometrischer Authentifikation funktioniert, insofern einen Vorteil bieten könnte, als die Unterwanderung des „Vier-Augen-Prinzips" dadurch faktisch unmöglich wird.

Abwehr 5: Rasche Reaktion im Ernstfall

Schließlich sind auch für den Ernstfall eines erfolgreichen Angriffs Maßnahmen vorzusehen, die eine rasche Reaktion ermöglichen. In diesem Zusammenhang sind zB im Vorfeld implementierte Möglichkeiten der kurzfristigen Beweissicherung von Kommunikationsdaten von erheblicher Bedeutung. Auch ein Leitfaden zum Umgang mit den involvierten Mitarbeitern, der insbesondere die Manipulation und Löschung relevanter Daten verhindern soll, kann die Aufarbeitung erleichtern.[1]

[1] Vgl näher *Fritzsche*, Eigenschaften von Fake President Fraud – Grundfragen zur Risikobeurteilung, Maßnahmenableitung und Reaktion im Einzelfall, Compliance-Berater 11/2017, 403–407..

Fazit

Der Fake President Fraud ist eine Betrugsmethode, die unvorbereitete Unternehmen schwer treffen kann, da die üblichen Abwehrmaßnahmen im Rahmen von Zahlungsfreigabe- und Kontrollsystemen den Tätern bekannt sind und daher gezielt umgangen werden. Ist man sich allerdings der Gefahr dieser Angriffe bewusst, können relativ simple Maßnahmen, die dem typischen Charakter des Fake Presdient Frauds gerecht werden, einen effektiven Schutz bieten und das Risiko, dass das Unternehmen Opfer eines derartigen Betrugs wird, beträchtlich reduzieren. Hervorzuheben ist dabei vor allem die zentrale Rolle der Mitarbeiter des Unternehmens: So reicht es nicht aus, dass ein Gefahrenbewusstsein bei den Verantwortlichen im Unternehmen besteht – vielmehr muss dieses auch auf jeder Hierarchieebene innerhalb des Unternehmens gelebt und deren Einhaltung auch in regelmäßigen Abständen überprüft werden.