Scam und Wire Transfer Fraud

Zunehmende Compliance-Risiken für den geschäftlichen Zahlungsverkehr

Das A und O eines gut funktionierenden Compliance Management Systems (CMS) ist dessen regelmäßige Überprüfung und Optimierung im Hinblick auf potenzielle Risiken. Hierbei dürfen nicht allein bisherige Unzulänglichkeiten des CMS in Bezug auf unternehmensinterne Risiken, sondern müssen insbesondere auch neue, von außen wirkende Entwicklungen bei der Einführung oder Anpassung präventiver und repressiver Compliance-Maßnahmen mitberücksichtigt werden. Der Beitrag verdeutlicht einige Gefahren die als „cybercrime" bezeichnet werden und gibt praktische Tipps sowohl für die Reaktion im Ernstfall, als auch für die effektive Vorbeugung.

Was ist Cybercrime?

Ein in den letzten Jahren weiter zunehmendes Risiko ist Cybercrime in all seinen Facetten. Unter dem Oberbegriff „Cybercrime“ werden alle Delikte zusammengefasst, die sich gegen das Internet, Datennetze, informationstechnische Systeme und deren Daten richten oder mittels dieser Informationstechnik begangen werden.

Typisch für diese Art von Straftaten ist ein sehr hohes Dunkelfeld von bis zu 90 % bei gleichzeitig sehr geringen Ermittlungserfolgen der Strafverfolgungsbehörden. Die Täter agieren dabei stets anonym, international vernetzt und gut organisiert.

Der durch Cybercrime jährlich verursachte Vermögensschaden bei Unternehmen beläuft sich allein in Deutschland auf einen hohen dreistelligen Millionen-Euro-Bereich; einige Schätzungen sprechen sogar von bis zu ca. 3,4 Milliarden €.[1]

Fokus: Scam und Wire Transfer Fraud

Eine momentan sehr verbreitete Art der Tatbegehung ist die im internationalen Bereich als „wire transfer fraud“ bzw. „fraudulent wire transfer“ bezeichnete Kombination aus Identitäts- und Überweisungsbetrug. Bei dieser Art der Tatbegehung legen es die Täter darauf an, die Opfer per E-Mail unter Verwendung einer erschlichenen Identität („scam“) zur Überweisung auf ein scheinbar sicheres, tatsächlich aber „betrügerisches“ Bankkonto zu veranlassen. Als potenzielles Opfer kann daher grundsätzlich jedes am Wirtschaftsleben teilnehmende Unternehmen in Betracht kommen, vom Kleinstunternehmen bis zum Großkonzern.

Der typische Ablauf

Das gesamte Vorgehen der Täter ist sehr raffiniert und mit einer eigenen Legende vorbereitet, ihre Informationen über das Unternehmen und die jeweiligen Beteiligten verschaffen sich die Täter unproblematisch aus dem Internet, aus sozialen Netzwerken oder gleich aus firmeninternen Datenbanken.

Dementsprechend sind die Betrugsmails professionell gestaltet, konkret adressiert und auf den ersten Blick von den bisherigen (echten) E-Mails des eigentlichen Geschäftspartners nicht zu unterscheiden. Von den allseits bekannten und massenweise versendeten, häufig plumpen Betrugsmails der „Nigeria-Connection“ sind sie weit entfernt. Erst eine genauere (zumeist im Nachhinein erfolgende) Überprüfung der E-Mail-Adresse des Versenders kann Zweifel hervorrufen, so etwa bei minimalen Buchstabendrehern.

Die Fälle aus der Praxis haben häufig den im Folgenden charakteristischen Ablauf.

1. Deliktsvorbereitung

Die später verwendeten Bankkonten werden nur wenige Tage vor der Kontaktaufnahme durch Hintermänner und nur für diesen einen Zweck eröffnet. Die wahre Identität der Hintermänner bleibt dabei verborgen: Soweit ersichtlich, handelt es sich bei diesen um ausländische Personen, die nur für die Konteneröffnung in ein bestimmte Zielland einreisen. Mithilfe einer Briefkastenadresse sowie eines gefälschten Reisepasses eröffnen diese sodann ohne weitere Probleme Konten in verschiedenen Währungen bei unterschiedlichen europäischen Großbanken.

2. Vertrauliche Kontaktaufnahme

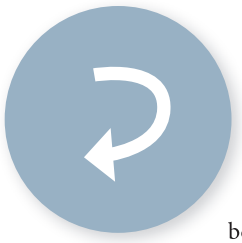
Der zuständige Sachbearbeiter, die im Unternehmen für Überweisungen zuständigen Personen oder sogar der Geschäftsführer des geschädigten Unternehmens erhalten von einem ihrer (zumeist ausländischen) Geschäftspartner eine an sie direkt adressierte E-Mail-Benachrichtigung, in der es um ein aktuelles Geschäft oder eine aktuelle Bestellung geht. Nicht selten arbeiten die Geschäftspartner seit mehreren Jahren (wenn nicht sogar einigen Jahrzehnten) zusammen und kennen sich daher auch persönlich. Um möglichst keine Zweifel hervorzurufen, werden z.B. auch Bezüge zu vergangenen gemeinsamen Projekten hergestellt oder man bedankt sich für das letzte persönliche Aufeinandertreffen im Rahmen einer Fachmesse o.Ä.

3. Aufforderung zum Überweisen

In Bezug auf das aktuelle Geschäft bittet der E-Mail-Versender schlüssig-glaubhaft um Überweisung der ersten Rate oder des gesamten Kaufpreises. Hierzu wird ein aktualisiertes Bankkonto benannt. Teilweise wird die Begründung für den Kontenwechsel gleich mitgeliefert und erscheint ebenfalls schlüssig zu sein. Um den Legitimationsanschein des neuen Bankkontos zu verstärken, kann der E-Mail sogar eine vom Vorstand des Geschäftspartners unterzeichnete Erklärung beiliegen, die den Kontenwechsel bestätigt.

Dr. Dominik Wagner, LL.M.

Der Autor ist Fachanwalt für Handels- und Gesellschaftsrecht sowie für Internationales Wirtschaftsrecht, Salary-Partner bei TIGGES Rechtsanwälte, Düsseldorf.



4. Durchführung der Überweisung

Aufgrund dieser Betrugsmails führt das geschädigte Unternehmen durch die befugte Person sodann die Überweisungen auf die benannten Konten aus. Diese Konten werden zumeist in einem anderen EU-Mitgliedstaat, jedoch bei europäischen Großbanken geführt. Dieser Umstand sorgt zusätzlich dafür, dass bei den Geschädigten kein erhöhtes Misstrauen erzeugt wird, das eine Überweisung unterbinden würde.

5. Geldabhebungen

Die Täter gehen auch bei der Leerung der Konten sehr raffiniert vor: Den staatsanwaltlichen Ermittlungsakten ist regelmäßig zu entnehmen, dass die Täter am Tag des Zahlungseingangs versuchen, soviel Geld wie nur möglich an allen möglichen Geldautomaten abzuheben und auch nicht davor abschrecken, die Gelder persönlich in Bankfilialen abzuheben.

6. Zeitverzögerte Aufdeckung des Delikts

Das vollendete Betrugsdelikt wird in den allermeisten Fällen erst mehrere Tage oder sogar erst mehrere Wochen nach seiner Vollendung festgestellt. Dies erfolgt häufig zusammen mit der Nachfrage des eigentlichen Geschäftspartners, wo denn die Zahlungen auf seine noch offenen Forderungen blieben. Bis dahin sind die Empfängerkonten aber zumeist schon leergeräumt und die geschädigten Unternehmen können sogar einen Totalschaden erleiden. Für solche Fälle kann sich eine entsprechende Versicherung als letzte Rettung erweisen.

7. Einstellung der Ermittlungen

Für die Ermittlungsbehörden sind die Hintermänner zumeist Phantome – es ist nicht bekannt, wer diese Personen sind und woher sie gekommen und wohin sie unmittelbar nach Tatbegehung wieder verschwinden. Demzufolge werden die Ermittlungsverfahren auch häufig nach nur kurzer Zeit vorläufig eingestellt.

Abhilfemaßnahmen gegen „Wire Transfer Fraud"

Sobald festgestellt wird, dass man Opfer eines Überweisungsbetruges geworden ist, ist die Devise „time is money" unbedingt wörtlich zu nehmen. Bei dieser Falschüberweisung geht es in erster Linie darum, noch möglichst viel von dem überwiesenen Betrag zurückzuerhalten. Ausgeschlossen ist dies keinesfalls, hängt aber entscheidend vom Reaktionszeitpunkt des Geschädigten ab. Folgende Maßnahmen sind empfehlenswert:

1 Kontakt mit der Hausbank
Zunächst sollte unverzüglich die eigene Hausbank über den Betrugsfall informiert und angewiesen werden, sich mit der Empfängerbank über das bankeninterne SWIFT-System in Verbindung zu setzen, um eine Blockierung des Empfängerkontos herbeizuführen. Die Erfahrung zeigt, dass diese Maßnahme am meisten Erfolg verspricht, den auf dem Konto noch vorhandenen Restbetrag zu retten.

2 Kontensperrung
Es ist zu erwarten, dass die Empfängerbank das Konto sodann vorübergehend blockieren und die zuständige Staatsanwaltschaft über den Vorfall in Kenntnis setzen wird.

3 Erstattung der Strafanzeige
Darüber hinaus sollte auf jeden Fall Strafanzeige gestellt werden, sowohl bei der für das geschädigte Unternehmen als auch bei der für die Empfängerbank zuständigen Staatsanwaltschaft. Es geht nur zweitrangig um die Hoffnung auf einen Ermittlungserfolg, sondern vielmehr um die Möglichkeit der späteren Akteneinsicht. Sowohl für die Versicherung als auch für die Vorbereitung möglicher Ersatzansprüche kann der Inhalt der Akten sehr interessant sein. Schließlich wird die örtliche Staatsanwaltschaft zumeist die Empfängerbank zur Rückzahlung des noch vorhandenen Betrages anweisen müssen, damit diese überhaupt tätig werden kann.

Weniger erfolgversprechend ist die direkte Kontaktaufnahme zur Empfängerbank, auch wenn man diesen Versuch trotzdem unternehmen sollte. Unter Verweis auf das Bankgeheimnis werden sich die meisten Banken jedoch in Schweigen hüllen.

Präventive Compliance-Maßnahmen: Allen voran – Sensibilisierung!

Aus der Perspektive der Compliance-Abteilungen ist jedoch viel spannender, entsprechende Vorbeugungsmaßnahmen zu treffen, um ähnliche Fälle zu verhindern, als auf den Ernstfall zu warten. Die Vorgehensweise der Täter ist häufig sehr ähnlich, die eingesetzten Methoden sind für diese Art der Tatbegehung charakteristisch. Dies erlaubt auch standardisierte Schutzmaßnahmen zu treffen, um die Erfolgswahrscheinlichkeit eines Überweisungsbetruges zu minimieren.

Da die Täter auch aufgrund einer gewissen Leichtfertigkeit ihrer Gegenüber so erfolgreich agieren können, wird es von ganz entscheidender Bedeutung sein, die im Unternehmen für Überweisungen verantwortlichen Personen für diese Art von Risiken überhaupt erst zu sensibilisieren. Insbesondere sollten diese dahingehend geschult werden, atypische Vorgänge als solche zu erkennen, zu überprüfen und im Bedarfsfall bestimmte Mechanismen einzuleiten.

Was im Einzelfall zu veranlassen sein wird, wird im Wesentlichen von der Struktur und den Prozessen des jeweiligen Unternehmens abhängen. Allgemein in diesem Zusammenhang können aber u.a. in Frage kommen:

- ✓ alle Zahlungsanweisungen auf neue Konten (auch scheinbar interne) lässt man sich von seinem Geschäftspartner persönlich telefonisch bestätigen,
- ✓ Einführung auch technischer Vorkehrungen zum Abgleich neuerer Korrespondenz mit älterer sowie des Versenders und seiner bisherigen E-Mail-Adresse,
- ✓ neue Geschäftspartner werden stets genauer überprüft, spätestens bei der ersten Überweisung,
- ✓ Einführung von Schutzmechanismen (Vier-Augen-Prinzip, Freigabe- oder Bestätigungsprozeduren) ab gewissen Beträgen und/oder bei ungewöhnlichen Zahlungsmodalitäten, wie auf vermeintliche Treuhandkonten.

FAZIT

Scam und Wire Transfer Fraud stellen für alle Unternehmen ein ernstzunehmendes Compliance-Risiko dar, weil grundsätzlich jedes Unternehmen einem Überweisungsbetrug zum Opfer fallen kann. Das Vorgehen der Täter wird immer raffinierter, sodass die betrügerische Absicht nur zu leicht verkannt wird. Die Folgen für die geschädigten Unternehmen führen nicht selten zu einem Totalausfall bei den überwiesenen Beträgen. Umso wichtiger ist es, dass Unternehmen ihr Personal für diese Art von Risiken sensibilisieren und entsprechende Vorbeugungsmaßnahmen einführen, die eine Verwirklichung dieser Risiken minimieren. Sofern der Ernstfall dennoch eintreten sollte, wird ein schnelles Reagieren von entscheidender Bedeutung sein.

1 Quelle: BKA, Bundeslagebild Cybercrime 2014; http://www.bka.de/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime__node.html.

Best Practice für Compliance und Sicherheit!

NEU!

comply.

Fachmagazin für Compliance-Verantwortliche

Als Compliance-Verantwortlicher haben Sie interdisziplinäre Aufgaben zu bewältigen und müssen jederzeit auf Unvorhersehbares vorbereitet sein. Mit der „comply." bringen der Bundesanzeiger Verlag und die Compliance Academy ein modernes Fachmagazin für Compliance-Verantwortliche in Unternehmen und Organisationen heraus. Erfahrene Kollegen und Kolleginnen aus unterschiedlichen Bereichen der Compliance sowie Experten aus Wissenschaft und Forschung berichten über bewährte wie neue Methoden zu Vermeidung und Bewältigung von Compliance-Risiken.

News, Diskussionen, Interviews und praktische Tipps, neue Trends und Entwicklungen aus dem In- und Ausland halten Sie in einem ansprechendem Format auf dem Laufenden. Jede Ausgabe vermittelt durch ein umfangreiches Autorenspektrum vielseitiges Erfahrungswissen. Die Vernetzung mit weiteren Informationsmedien und Veranstaltungen bietet Ihnen die optimale Fortbildung.

ISSN 2364-7604
Fachmagazin, ca. 48 Seiten, Format A4,
4 Ausgaben im Jahr, Jahresabonnement
inkl. Online-Archiv
129,00 €
Preise inkl. MwSt. und Versandkosten
(deutschlandweit)

IHRE VORTEILE

- schneller Erfahrungstransfer und hilfreiche Management-Tipps
- innovative Compliance-Methoden
- kompakte Darstellung fachübergreifender Themen und der Entwicklung von Compliance
- aktuelle Zusammenfassung von Rechtsprechung und Gesetzesänderungen
- schnell zu erfassende und leicht zu lesende Fachbeiträge im modernen Layout
- weitere vernetzte Informationsmedien zur Wissensvertiefung

INHALT

- Brennpunktthemen
- News
- Diskussionen
- Interviews und praktische Tipps von Experten
- neue Trends und Entwicklungen aus dem In- und Ausland rund um Compliance.

AUTORENINFO

Herausgegeben vom Bundesanzeiger Verlag und der Compliance Acadamy unter der Schriftleitung von Prof. Dr. Bartosz Makowicz, Europa-Universität Viadrina Frankfurt an der Oder

Bundesanzeiger Verlag
www.bundesanzeiger-verlag.de

Jetzt versandkostenfrei (deutschlandweit) bestellen:
www.comply-online.de
E-Mail: wirtschaft@bundesanzeiger.de
Telefon: 0221/97668-315 · Fax: 0221/97668-271
in jeder Fachbuchhandlung

BESTELLSCHEIN

→ www.comply-online.de

→ **E-Mail**: wirtschaft@bundesanzeiger.de
→ **per Telefon:** 02 21 / 9 76 68-315
→ **per Fax** an 02 21 / 9 76 68-271
→ in jeder **Fachbuchhandlung**
→ im **Fensterkuvert** einsenden an:

Bundesanzeiger Verlag
Postfach 10 05 34
50445 Köln

Best Practice für Compliance und Sicherheit!

Ja, hiermit bestelle ich

☐ die **Zeitschrift „comply."** inkl. Online-Archiv für ..... 129,00 €
inkl. Versand und MwSt. (Jahresabonnement für 4 Ausgaben im Jahr)

☐ die **Zeitschrift „comply."** inkl. Online-Archiv
zum Sonderpreis von nur ..... 98,00 €
inkl. Versand und MwSt. (Jahresabonnement für 4 Ausgaben im Jahr)

- ☐ Ja, ich beziehe bereits eine der folgenden Zeitschriften: AW-Prax, FuS, BOARD
- ☐ Ja, ich bin Mitglied bei DICO, BCM, BUJ, AdAR, Netzwerk Compliance e.V. oder BDCO
- ☐ Ja, ich arbeite bei einer Behörde

ABSENDER:

Firma

Name, Vorname

Straße, Nr.

PLZ, Ort

Telefon | Fax

E-Mail – wichtig bei der Bestellung von Online-Produkten und Produkten inkl. Online-Archiv

☐ **Ja,** ich möchte kostenlos über Neuerscheinungen, Angebote und Aktionen per E-Mail auf dem Laufenden gehalten werden. Diese Zustimmung ist freiwillig und kann jederzeit unter vertrieb@bundesanzeiger.de widerrufen werden.

Datum, Unterschrift

VIELEN DANK FÜR IHRE BESTELLUNG!

11003520

Deutschlandweit Versandkostenfrei!

Versandkostenpauschale europaweit 4,00 €, weltweit 8,00 €

Jetzt 4 Wochen unverbindlich und kostenlos testen!

IHRE ZUFRIEDENHEIT – UNSERE GARANTIE

Sie bestellen bei uns zur Ansicht und können unsere Produkte, ausgenommen CD-ROMs, DVDs, Online-Datenbanken und E-Books, zunächst kostenlos testen. Sollten Sie nach Prüfung wider Erwarten nicht zufrieden sein, senden Sie das Produkt einfach zurück – weiter brauchen Sie nichts zu unternehmen.

VERBRAUCHERSCHUTZHINWEIS:

Bitte beachten Sie unsere AGB sowie die Widerrufsbelehrungen auf unserer Webseite: shop.bundesanzeiger-verlag.de/agb.

DATENSCHUTZHINWEIS:

Ihre Daten sind bei uns in sicheren Händen! Informationen zu unseren AGB und Datenschutzbestimmungen finden Sie unter www.bundesanzeiger-verlag.de.

Ihre Bundesanzeiger Verlag GmbH

www.bundesanzeiger-verlag.de

Bundesanzeiger Verlag