KPMG

KPMG Indonesia Advisory Newsletter

April 2017

#1 不正被害事例「ビジネスメール詐欺」

皆さんは、「Business Email Compromise(BEC)」や「ビジネスメール詐欺」という言葉を耳にしたことはありますか。BECとは企業を標的としたEメール詐欺で、米FBIの統計*1では、全世界での被害件数は2万件を超え、被害金額も約31億米ドルに達していると報告されています。近年、インドネシアでも被害が拡大しており、注目が集まっている不正の手口です。

本稿では、ビジネスメール詐欺の典型的な手口と被害事例を紹介し、企業に求められる対応策について解説します。

*1 https://www.ic3.gov/media/2016/160614.aspx

1. ビジネスメール詐欺の特徴

ビジネスメール詐欺は、「ホエーリング(捕鯨)」や「CEO詐欺」とも呼ばれる詐欺で、大量のメールを送信するフィッシングとは異なり、ターゲットを絞りこみ、企業の組織や支払いプロセスなどの内部情報を徹底的に調べて仕掛けてくることが特徴です。

また、不正プログラムを利用するケースもありますが、多くの場合はソーシャル・エンジニアリング(ウィルスや不正ウェア等を用いず、人間の心理的な隙や行動特性につけこみ、機密情報を入手するなどの不正を働く手法のこと)が駆使されるため、セキュリティ・ツールなどでは防止・発見が難しく、世界中で被害が拡大しています。

2. 典型的な手口

- タイプ①:「幹部社員へのなりすまし」

  幹部社員になりすまし、ターゲット企業の従業員に対して、緊急の送金依頼や情報提供を求めるケース
- タイプ②:「取引先企業へのなりすまし」

  取引先企業の社員になりすまし、ターゲット企業の購買担当者または支払担当者に対して、支払先を偽造した偽の請求書を送付してくるケース
- タイプ③:「アカウントの乗っ取り」

  メールアカウントなどを乗っ取り、ターゲット企業の顧客に対して、偽造した請求書・支払依頼メールを送信するケース

3. 被害事例

事例①: 海外出張中の社長からの緊急送金の指示

経理部門長は、海外出張中の社長(なりすまし)から、緊急で送金が必要になった旨のメールを受信した。そのメールには、対応の可否に加えて、送金手続きの例外対応についても連絡するように記載されていた。

経理部門長が例外対応できる旨及び対応方法について返信すると、社長(なりすまし)から、送金先の口座と「PCにアクセス出来次第、請求書を送付するので、直ちに送金処理をするように」と連絡があった。

経理部門長は、部下である担当者に送金準備をすすめるよう指示し、経理担当者は指示内容に従い、ネットバンキングシステムに支払情報を入力した。経理部門長は、その内容を確認・承認し、緊急時の承認者に設定していた他の幹部社員にも手続きをすすめるように連絡し、そのまま犯人の口座への支払いを完了させた。

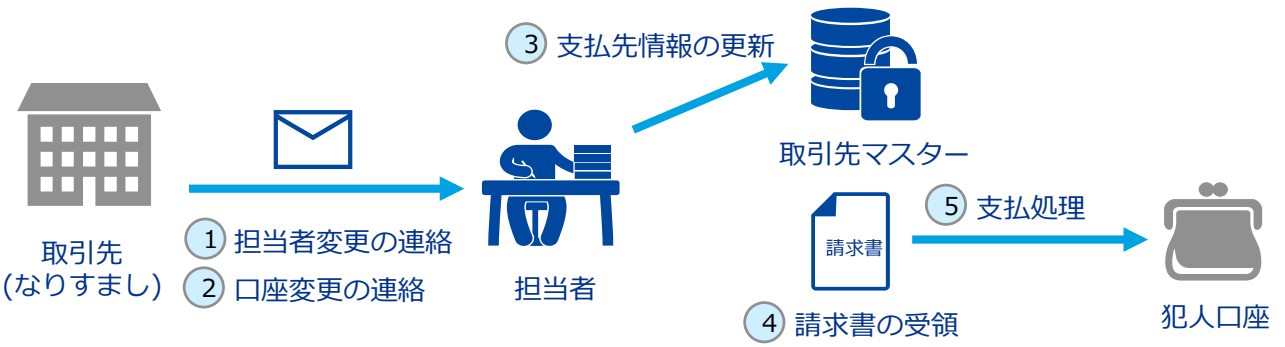
完了した旨を、念のため社長の会社メールアドレスもCCに入れて連絡したところ、社長から電話があり、騙されていたことが発覚した。

補足:メールアカウントを乗っ取らずに、一文字違いなどのメールアドレスから連絡してくるケースや海外出張中であるために会社のメールにアクセスできないことを理由にフリーメールカウントから連絡してくるケースもある。メールの文末に、“Sent from my iPhone”など個人用端末から送っていることを装うなど、信憑性を高めるための様々な細工がされているため、なりすましであることを見抜けないケースが多い。

事例②: 取引先からの支払口座変更の連絡

取引先(なりすまし)から担当者変更のメールを受けた数ヶ月後に、取引先の新しい担当者から次回の支払いから支払口座を変更したい旨のメールを受信した。念のため、数ヶ月前に受信していたメールに記載されていた電話番号に確認の電話を入れたところ、変更依頼のメールを送信したことが確認できたため、取引先マスターの登録情報の変更手続きを進めた。

それ以降、請求書を受領する度に、新たに指定された口座に支払いを行っていたが、入金が滞っていることを不審に思った取引先から連絡があり、騙されていたことが発覚した。



4. 企業に求められる対応策

ビジネスメール詐欺の特徴は、人間の心理的な隙や行動特性につけこみ、企業のセキュリティ対策や不正防止対策を突破するという点にあります。入手した従業員情報や社内プロセスなどの会社情報を活用したり、メールなどのやり取りを通じて信頼関係を構築するなど、疑われにくいシュチュエーションを作り上げた上で仕掛けてきます。

企業がビジネスメール詐欺から身を守るためには、以下のような対策が効果的です。

- 「2段階認証の導入」メールだけのやりとりではなく、通常使用している電話番号に連絡し、指示・依頼内容の確認を行う。
- 「従業員に対する意識付け」従業員はセキュリティという観点からは最も脆弱な侵入経路となり得ます。セキュリティ教育等を通じた従業員の感度を高めることが重要です。
- 「被害事例の収集」犯罪者の手口は日々進化するため、他社の被害事例の収集を通じて手口を理解することが重要です。被害事例を踏まえ、自社での発生可能性をチェックすることは、防止・早期発見に向けて有用です。

本件に関連する弊社サービス

■ビジネスメール詐欺被害診断

[支援内容]

最新の被害事例などを踏まえた想定シナリオに基づき、過去の支払いデータなどを解析し、ビジネスメール詐欺の被害の確認・被害状況の把握を支援いたします。現行の組織・業務プロセスにおける脆弱性の診断や当該テーマに関する内部監査の実施支援、従業員の意識向上に向けたトレーニング等も支援可能です。また、サイバーセキュリティーなども加え、貴社の情報セキュリティ態勢について包括的なチェックを行うことも可能です。

詳細は、以下にお問合せください。

KPMG Siddharta Advisory
35th Floor, Wisma GKBI
28, Jl. Jend. Sudirman
Jakarta 10210, Indonesia
電話: +62 (0) 21 574 0877
ファックス: +62 (0) 21 574 0313

Ho Wah Lee
Head of Advisory Services
Wahlee.ho@kpmg.co.id

蓑和 秀夫
Hideo.Minowa@kpmg.co.id

kpmg.com/id