事例で学ぶセキュリティインシデント（第6回）

危うく引っかかるところだったビジネスメール詐欺

2023.11.16

海外の取引先から変な請求書がメールで送られてきたのですが、見てもらえますかーー。経理から、F社の情報システム担当者に声がかかったのは休み明けの月曜日朝のことだ。情報システム担当者がメールを確認すると、“取引先”と称する相手からの請求書と振込先の銀行口座番号ともに次のような文面が添えられていた。「新たに御社専用の銀行口座を設けたので、今回から新しい口座に振り込みをお願いします」。このメールを読んだ後、情報システム担当者は「これはビジネスメール詐欺ではないか」と直感した。

送金口座の変更は要注意

ビジネスメール詐欺とは、攻撃者（犯罪者）が取引先や自社の経営者などになりすまし、偽のメールを送りつけ、攻撃者が用意した口座に送金させる詐欺の手口で、サイバー攻撃の1つだ。主な攻撃の手口は、取引先の担当者になりすまして偽の請求書などを送り、偽の口座に送金させるというもの。

攻撃者は、請求書の内容に間違いがあったので、改めて送ると　をついたり、従来の口座が金融機関の都合で使用できなくなったので新しい口座に送金してほしいなどと言ったり、さまざまな理由を付けて振込先の変更を伝えることも常とう手段だ。また、自社の経営者などになりすまし、「秘密裏に企業買収の話し合いを進めており、買収の手付金が急に必要になった」など、もっともらしい偽のメールを役員や経理担当者に送り、偽の口座に送金させるなどの手口もある。攻撃者は事前に経営者や経理担当者のメールアカウントを盗み取り、あたかも社内のメールであるかのように装うので引っかかる危険性がある。

さらに悪質な手口もある。資材調達など実在する部門の担当者のメールアカウントを乗っ取り、取引先に偽の請求書と口座情報のメールを送り付け、金銭を振り込ませる。メールに記載される送信元の名前やメールアドレスが本物であるため、受信者はメールを悪用した詐欺であるとは気付きにくく、偽の口座に送金してしまう恐れがある。

怪しい請求書は直接担当者に確認する

ビジネスメール詐欺を防ぐ第一の方法は、メールを悪用した詐欺のリスクがあるのを理解することだ。その上で、請求書や支払先の銀行口座が通常と異なるなど詐欺が疑われる場合、送信元の取引先の担当者に確認する。

攻撃者から送られてきたメールをそのまま返信したり、メールに記載された携帯電話番号に電話したりすると、攻撃者にだまされる恐れがある。そのため、取引先の担当者や上司の名刺などで電話番号を確かめたり、取引先の代表電話に電話をかけたりして担当者本人に直接内容を確かめるといった手順が必要だ。

取引先のメールアドレスに似せた偽のメールアドレスが使われることもある。攻撃者は正規のメールアドレスの文字を入れ替えるなど、ちょっと見ただけでは偽のメールであることが分からないようにする。メールの内容が疑われる場合、メールアドレスが本物かどうか疑い、確かめる必要がある。

そして、ウイルス対策と同様に「不審なメールの添付ファイルは開かない」「攻撃者に不正利用されないように複雑なパスワードを設定する」「ウイルス対策ソフトやパソコンの基本ソフト（OS）は最新の状態に更新する」などの基本的なセキュリティ対策をきちんと講じる点も大切だ。

取引先のメールが攻撃者に盗み取られた

では、冒頭で紹介したF社の話に戻そう。同社は、アジアをはじめ海外のさまざまな国・地域から生活雑貨などの商品を輸入している。買い付けは商品企画部門の担当者が年に数度、出張したり、日本語が通じる現地のバイヤーに依頼したりして競合の卸売業とは一線を画すユニークな商品を取り扱ってきた。

同社の情報システム担当者は管理部門を兼務しているが、セキュリティを含めたITの構築・運用を担っている。連絡してきた経理担当者も同席し、最初にメールを受け取った商品企画部門の担当者に経緯を聞いた。請求書の内容は特におかしなところはなく、送金先の口座番号の変更についても疑いを持たずにいつものように請求書を経理担当者に回したという。

経理担当者が送金先の銀行口座の変更を不審に思い、情報システム担当者に相談したことで、今回のインシデントが発覚した。経理担当者が現地のバイヤーに口座変更の理由を確認したところ、そのような事実はなく、詐欺メールであることが明らかになった。

ただ、請求書の内容については、バイヤーのメールが攻撃者に盗み取られた可能性があり、情報システム担当者はその旨をバイヤーに伝え、セキュリティ対策の強化を依頼した。

幸いにもビジネスメール詐欺の被害を未然に防いだものの、情報システム担当者はインシデント経緯について経営層をはじめ全従業員に伝え、メールの取り扱いについて改めて注意を促した。具体的には、取引先からの請求書や注文書などに限らず、不審なメールを受け取った場合、上司や情報システム担当者に報告するなどのルール徹底を通達した。また、攻撃者は乗っ取った正規のメールアカウントを悪用してメールサーバーに不正アクセスし、取引先とのやり取りを盗み見るリスクもあるため、メールアカウントのパスワードを推測されにくいものにしたり、定期的に変更したりすることも注意喚起した。そして、攻撃者のなりすましを防ぐため、送信元の身元を証明する電子署名などの導入を検討することとした。

メールは業務に欠かせない社内・社外とのコミュニケーション手段だ。しかし、メールを悪用した標的型メール攻撃やウイルスの感染経路になるリスクがあり、メールだけに頼らない情報のやり取りを考える必要がある。F社では、社内・社外とファイルをやり取りする手段としてクラウドストレージの導入を検討し、商品カタログなどメールでの送受信が難しい大容量データや、商品の発注書・請求書などの重要な文書についても、安全にやり取りが実現する環境の構築に向けて取り組みを模索している。