潜行するサイバー攻撃（第1回）

“企業版”オレオレ詐欺が横行

2017.05.31

子どもや孫になりすまして金銭をだまし取る「オレオレ詐欺」や、融資の保証金などの名目で金銭を振り込ませる「融資保証金詐欺」など、振り込め詐欺が社会問題になっている。この“企業版”オレオレ詐欺といえるのが「ビジネスメール詐欺」だ。

国内でもビジネスメール詐欺が発生

ビジネスメール詐欺は、偽メールを企業に送りつけ、役員や従業員をだまして送金させる新手のサイバー攻撃だ。米連邦捜査局（FBI）の報告によれば、ビジネスメール詐欺の被害額は約31億ドルに及ぶという。すでに世界中で約2万2000社が被害に遭っている。

日本でもビジネスメール詐欺の被害が発生している。全国銀行協会では「法人間の外国送金の資金をだまし取る詐欺にご注意！」とインターネットで告知。国内で発生した事案は、「外国法人になりすまして送信された電子メールの送金指示」に従ったというもの。「電子メールまたは添付請求書が改ざんされ、本邦法人の指示口座とは異なる口座に送金された」というケースもあった。

対策としては、「通常の請求・支払慣行と異なる対応を求められた場合は、外国法人に対して、送金前に電子メールとは異なる手段（電話やFAX等）で事実の確認を行う」。また、パソコンの情報セキュリティー対策も必要だという。

ウイルス対策やスパム対策などを適切に実施

(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start': new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0], j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src= 'https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f); })(window,document,'script','dataLayer','GTM-K9XWQF5'); !function(f,b,e,v,n,t,s) {if(f.fbq)return;n=f.fbq=function(){n.callMethod? n.callMethod.apply(n,arguments):n.queue.push(arguments)}; if(!f._fbq)f._fbq=n;n.push=n;n.loaded=!0;n.version='2.0'; n.queue=[];t=b.createElement(e);t.async=!0; t.src=v;s=b.getElementsByTagName(e)[0]; s.parentNode.insertBefore(t,s)}(window, document,'script', 'https://connect.facebook.net/en_US/fbevents.js'); fbq('init', '996021997138363'); fbq('track', 'PageView'); var yahoo_retargeting_id = 'R26PZOZHRX'; var yahoo_retargeting_label = ''; var yahoo_retargeting_page_type = ''; var yahoo_retargeting_items = [{item_id: '', category_id: '', price: '', quantity: ''}]; /*]]> */ window.dataLayer = window.dataLayer || []; function gtag(){dataLayer.push(arguments);} gtag('js', new Date()); gtag('config', 'AW-686888305');

こうした状況の中、情報処理推進機構（IPA）技術本部セキュリティセンターでは2017年4月、「ビジネスメール詐欺」に関する事例と注意喚起のレポートを公表し、主な手口を5つのタイプに分類した。

●タイプ1：取引先との請求書の偽装
●タイプ2：経営者等へのなりすまし
●タイプ3：窃取メールアカウントの悪用
●タイプ4：社外の権威ある第三者へのなりすまし
●タイプ5：詐欺の準備行為と思われる情報の詐取
（※『ビジネスメール詐欺「BEC」に関する事例と注意喚起』P4から引用）

いずれのタイプも、自社の社長や取引先、弁護士など、メールを受信した担当者がつい信用してしまう相手になりすますのが特徴だ。攻撃者が従業員のメールアカウントを乗っ取って、取引先に偽の請求書を送る手口もある。

ビジネスメール詐欺を防ぐには、従来の情報セキュリティー対策を適切に行うことだ。例えばメールの本文や添付ファイルに含まれる不正なプログラムを検知・駆除するウイルス対策や、迷惑メールをブロックするスパム対策、怪しいWebサイトへのアクセスを制限するURLフィルタリングなどの対策は基本といえる。さまざまな情報セキュリティー機能を1台の機器に統合したUTMも活用するとよい。

加えて、メールアカウントに使用するパスワードは定期的に変更する、類推されやすいものは避ける、生体認証などを組み合わせた二要素認証を採用するといった対策も有効だ。また、特定の組織・個人を狙う標的型攻撃メールの対策と同様に、件名や送信元が不明なメールは開かない、メールの本文に記載されたURLはむやみにクリックしない、メールの取り扱いについて定期的に情報セキュリティー研修を行うなどの取り組みも欠かせないだろう。

オレオレ詐欺の場合、高齢者に対する銀行窓口での“声掛け”が被害を未然に防ぐケースもある。ビジネスメール詐欺についても、狙われやすい財務や経理担当者の情報セキュリティーに対する意識向上が欠かせない。自分宛ての送金依頼メールであっても、正規なものかどうかいったん疑い、部門内で確認し、場合によっては経営層に報告してから処理するといった自衛策を考えたい。