セキュリティ

ITマネジメント（内部統制）

“人の脆弱性”を狙った攻撃が増大、日本でも被害が

その社長は本物ですか？ “なりすまし”で億単位の金銭を奪う「BEC」

サイバー攻撃の手法は日々進化しており、昨今では“人の脆弱性”を狙ったソーシャルエンジニアリングの手法を組み合わせた攻撃が使われるようになってきました。その代表例といえるのが「BEC：ビジネスメール詐欺」です。この攻撃ではあらかじめメールシステムに侵入し、社内のメールのやり取りを把握した上で、タイミングを見計らって“なりすましメール”を送信し、金銭や情報を奪います。今回は、BECのしくみと対策についてご紹介します。

莫大な被害を生むビジネスメール詐欺（BEC）

取引先や自社の経営層などになりすまして送金指示のメールを送り、金銭を詐取する手法を「ビジネスメール詐欺：Business Email Compromise（BEC）」と呼びます。ビジネスにおけるコミュニケーションの主流が、電話からメールに変わったことを悪用した手法といえます。

海外では数年前からBECの被害が増大しており、FBI（米連邦捜査局）が発表したレポートによると、2013年10月から2016年5月までの2年半ほどの間に1万5千件以上、被害額は10億5千万ドルに上るとされています。さらにその後の発表により、2018年5月までの累計被害は、米国で7万9千件弱、被害額は125億4千万ドル近くまで拡大しています。まさに桁違いの被害額といえましょう。そして2017年からは、日本でも同様の手口による被害が確認されています。

BECの手法は、取引先などになりすまして偽の請求書を送るものと、社内の経営層などの内部になりすまして送金指示メールを送るものの大きく2つに分けることができます。IPA（独立行政法人情報処理推進機構）ではこれをさらに細分化し、「取引先との請求書の偽装」「経営者等へのなりすまし」「窃取メールアカウントの悪用」「社外の権威ある第三者へのなりすまし」「詐欺の準備行為と思われる情報の詐取」の5つのタイプに分類しています。日本でも徐々に被害が増えており、2018年夏には日本語によるBECも確認されました。

IPAのほかにも、警察庁や警視庁、一般社団法人 全国銀行協会などが注意喚起を行っていますが、かなりの数の組織がBECメールを受け取っている可能性があり、攻撃に気づいていないケースも多いと思われます。ただし最近では、BECにより多額の被害を受けた事例がニュースなどで広く取り上げられたこともあり、後で「実は被害を受けていた」と気づくことも増えているようです。

社内のやりとりをモニターし、最適なタイミングでメールを送信

BECは、なりすましというシンプルな手口ながら、周到に計算された攻撃です。BECを行うサイバー攻撃者は、まず標的となる企業について情報収集を行います。ドメインや名刺などからその企業が使っているメールアドレスは容易にわかるので、そこから経営層や経理担当のメールを類推し、判明したら今度はパスワードを入手します。辞書攻撃などでパスワードを割り出すこともできますし、フィッシングメールやキーロガーを活用することもあります。

メールシステムに侵入できたら、そこでやり取りされるメールから取引先やその担当者、送金される名目などの情報を集めていきます。定期的な送金を行っている取引先を見つけると、タイミングを見計らって取引先になりすまし、「振込先の口座を変更した」などといった内容のメールを送るのです。また、メールのやり取りから企業の買収の話が進んでいることがわかれば、経営層になりすまして、買収がまとまりそうなタイミングなどに、送金先を指示する内容のメールを送ります。

サイバー犯罪者がBECのメールを送る際には、メールにさまざまな細工を施します。文体はなるべく本物に似せて書きますし、メールの署名も本物と瓜二つのものを作成します。送信者や返信先のメールアドレスなどといったヘッダー情報も一目ではわからないように偽装します。さらに、サイバー攻撃者が標的となる人物のPCを乗っ取り、そのPCをリモートコントロールしてメールを送ることもあります。これは本人からのメールということになるので、受け取った側が気づくことはかなり困難といえます。

BEC対策には、システムとアナログの併用が効果的

BECはマルウェアの類を一切使用せず、ソーシャルエンジニアリングの手法のみで莫大な金銭や重要な情報を得ることができるため、その数は増える一方です。そのため、前述のように入念な準備を行うものだけでなく、公開情報を元にした安直なBECも見受けられるようになりました。このように安直なBECであれば、本文やメールのヘッダーなどをチェックすることで、容易に見破ることができるでしょう。また、入念に準備されたBECであっても、システムと人の両面から対策を行うことで、BECに気づく可能性が高くなります。

具体的には、送金や重要な情報を送信する際の社内ポリシーを策定することから始めます。例えば、一定額を超える送金処理を行う場合には、複数の役職で稟議を通すようにする、振込先の変更があった場合には、送金先に電話をするなどして本人確認を必ず行う、メールだけでなく書面も必要とする、といったところです。もちろん、従業員にセキュリティ教育を実施することも重要になります。

システム面での対策としては、メールに送信者ドメイン認証（DKIM、SPF、DMARC）を導入することで、不正なメールサーバによるドメイン詐称メールを検知することができます。また、登録された口座以外への振込を禁止するなど、システム上で制約を設けることも効果的です。こうした対策には、例えばNTT Comが提供する「WideAngle マネージドセキュリティサービス」の「コンテンツセキュリティ」や「コンサルティング」などが活用できます。なお、ソーシャルエンジニアリングの手法を使った攻撃はBECだけではありません。いわゆる「ばらまき型」のスパムやフィッシング詐欺などでも使われる手法なので、これらについても併せて対応が必要です。

関連サービス

WideAngle マネージドセキュリティサービス	ファイアウォールやIPS/IDS、アンチウイルスなど、ご要望の高いネットワークセキュリティやコンテンツセキュリティを一括してアウトソーシングできるパックメニューです。 セキュリティ運用基盤（SIEM）とリスク分析官による相関分析で、ファイアウォールなど機能単体での運用では気がつかない未知の脅威をあぶりだします。
WideAngle プロフェッショナルサービス	経験豊富なセキュリティエキスパートが企業のリスクマネジメントにおける現状と課題を抽出し、解決に導くソリューションです。グローバル統一手法によりセキュリティリスクを調査・把握し、改善からモニタリングまで総合的にサポートする「コンサルティング」、セキュリティインシデント発生時における被害拡大防止や復旧支援を行う「レスキューサービス」、ICT環境の弱点を可視化する「脆弱性診断」で構成されます。