セキュリティ

ITマネジメント（内部統制）

誰もが引っかかってしまうソーシャルエンジニアリング

最新のフィッシング詐欺は システムと教育の組み合わせで防ぐ

フィッシング詐欺やBEC(ビジネスメール詐欺)といった、ソーシャルエンジニアリングの手法を使用したメール攻撃が急増しています。これらは、人間心理の隙を突くため、受け手側もうっかりひっかかってしまうことが多くなっています。こうした攻撃には複数の対策を組み合わせることや、教育によって従業員のセキュリティ意識を高めることが効果的とされています。今回は、NTT Comの総合リスクマネジメントサービス「WideAngle」を例に、フィッシング詐欺対策について解説します。

急増するフィッシング詐欺

フィッシング詐欺は、実在する金融機関やサービスなどに見せかけてIDやパスワードなどの機密情報を盗み出そうとする詐欺で、似たような詐欺は古くからありました。それがインターネットの普及により、メールやWebサイトを利用するようになったことから、「洗練された手口(sophisticated)」と、「釣る(fishing)」を掛け合わせて「フィッシング詐欺(phishing)」と呼ばれるようになりました。現在ではさらに手法が洗練されてきており、企業の経営層や取引先になりすまし送金指示のメールを送る「BEC：Business Email Compromise(ビジネスメール詐欺)」が急増しています。

フィッシング詐欺は、実在するWebサイトにそっくりの偽サイトを用意し、メールを使ってユーザーを誘導、IDとパスワードなどを入力させて、その情報を盗み取るという手法です。この攻撃には人間心理の隙を突くソーシャルエンジニアリングの手法が用いられており、たとえば銀行やカード会社を装って「不正なログインを検知したのでアカウントを停止した」「新たなセキュリティ対策を導入した」などという内容のメールを送り、偽サイトへのリンクをクリックさせようとします。他には、オンラインゲームからのお知らせや宅配便の不在通知、ショッピングサイトからの購入確認などになりすますケースも見受けられます。こうしたメールのほとんどは受け手側を焦らせる内容となっており、多くの人が騙されてしまうのです。

ここにきてフィッシング詐欺は急増しており、さまざまな種類の偽サイトが見られるようになりました。以前は海外からの攻撃が多いせいか、おかしな日本語を使ったものが多かったのですが、最近では違和感のない文章を駆使するようになっており、受け手が引っかかる可能性も高まっています。

フィッシング詐欺によって盗み取られたログイン情報は、アンダーグラウンドの市場で売買され、不正アクセスや他のサービスへのログイン試行に悪用されるのです。また、この種の市場ではサイバー攻撃者向けにフィッシング詐欺に使うツールやクラウドサービスが提供されており、誰でも簡単にフィッシング詐欺が行えるようになっていることも、増加の背景にあると思われます。

URLフィルタリングで偽サイトへのアクセスをブロック

こうしたフィッシング詐欺への対策としては、第一にメールの送信元や返信先の確認が考えられます。これらの表示は送信者が自由に変更できますが、メールのヘッダー情報を参照することで本来の設定を調べられます。しかしサイバー攻撃者もそのあたりは承知しており、正式なサービスとまぎらわしいドメイン名を使用します。例えば、画面の文字サイズが小さいと小文字の「l」(エル)と大文字の「I」(アイ)、数字の「1」の見分けは困難でしょう。こうした文字を使って正規ドメインにそっくりの偽ドメインを仕立てるわけです。

別の対策としては、メールに送信者ドメイン認証(DKIM、SPF、DMARC)を導入して、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というものです。ただし、受信者だけでなく送信者もドメイン認証のしくみを導入する必要があるため、前述の偽ドメインへの対応は難しいとされています。

システムによる対策としては、リンクをクリックしたときにそのWebサイトの安全性をチェックするURLフィルタリングが効果的でしょう。URLフィルタリングは、Webサイトの情報を収集し、ジャンル別に分類したり、安全なもの／危険なものなどのようにリスト化したりします。

また、過去に改ざんされたことがあったり、マルウェア配布サイトとして使用されたりしたWebサイトのURLの情報も、IPアドレスまで含めて収集しており、これらのサイトへのアクセスを制限することもできます。これらの機能により、例えユーザーがフィッシング詐欺のリンクをクリックしてしまったとしても、すでに偽Webサイトということが明らかになっていれば、アクセスをブロックしてくれます。NTT Comの「WideAngle マネージドセキュリティサービス」では、コンテンツセキュリティ機能の1つとして前述したようなURLフィルタリングを提供しています。

フィッシング詐欺を見抜く力を育てる

フィッシング詐欺メールは、冷静にメール内容を確認すれば騙される確率はぐっと低くなります。なぜなら、その多くは「ばらまき型」といって、不特定多数に送信されるものだからです。正式なメールであれば、文面の冒頭などにユーザー名や会員番号などが表示されている場合が多いのですが、フィッシング詐欺のものにはそれがないことがほとんどでしょう。また、本来メールの末尾にあるべき送信元の署名がないこともしばしばです。文面も、日本語のおかしなところがないように見えても、顧客に送る文章では使わない表現や言い回しが見つかるかもしれません。

しかしフィッシング詐欺のメールは、アカウント停止や不正ログインなどのような件名や文面に「至急」などの文言を加えることで、受け手の冷静さを失わせようとします。よってフィッシング詐欺へ対抗するためには、システムだけでなく、人の面での対策、すなわちセキュリティ教育も重要となるのです。教育により各ユーザーのリテラシーを向上させることで、フィッシング詐欺に引っかかる確率を下げることができるでしょう。

例えば、NTT Comが提供する「WideAngle プロフェッショナルサービス」では、コンサルティングサービスも提供されており、教育も含まれています。教育には、フィッシング対策のしくみや手法といった基本的なものから、BECやスピアフィッシングといった最新の攻撃手法まで対応するほか、実際に疑似メールを送信し、メールを開いたり本文にあるリンクをクリックしたりした人が何人いたかなどを調査。該当する人に再教育を行うなど、基本から実践まで多彩な教育メニューが用意されています。

また、教育の実施方法についても、全社一括、部署単位、個人などで実施するもの、外部から講師を招くもの、講習用のスライド資料を使用するもの、インターネットの教育コンテンツを受講するものなど、さまざまな実施スタイルから選ぶことができます。

このように、フィッシングメールやBECといったソーシャルエンジニアリングの手法を活用した攻撃については、システムと教育の両面から対策を行うことが重要です。会社と従業員を守るためにも、各種サービスの活用を検討してみてはいかがでしょうか。

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。