Case study

公益事業会社、フィッシング感受性（フィッシングメールにより影響され易い状態）を67%以上低減!

WombatのThreatSim®によるミュレートされたフィッシング攻撃は、組織全体におけるセキュリティ対策の改善に役立ちました。

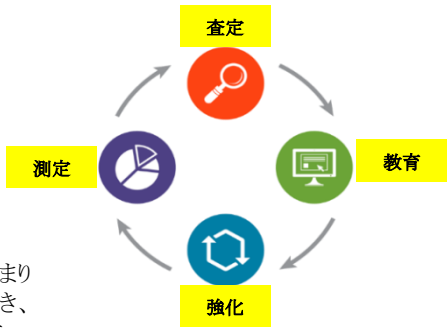
課題

2013年、米国西部に拠点を置く某大手公益事業会社は、事実上、全ての組織(重要インフラ内外の組織)が、フィッシング攻撃を認識する方法を理解しておらず、エンドユーザに関わる可能性がある、という問題を抱えていました。

サイバーセキュリティに対する意識や理解、及びトレーニングを担当する当組織の情報セキュリティスペシャリストは、「2013年当時、フィッシング脅威は今ほど深刻ではありませんでしたが、当社が問題を抱えていることは確実に分かっていました」と述べています。「また、問題は悪化する可能性しかないということが分かっていました」

トレーニングマネージャの話では、幸いなことに、彼女とサイバーセキュリティチームは、フィッシング判定プログラムを開始するための賛同を得ることができました。
「問題に対処する必要があることに上層部が同意したので、非常にうれしく思いました」

Wombatの継続的トレーニング方法



ソリューション

プログラムの配信・管理だけでなく結果の測定も行うための適切なプラットフォームの調査が始まりました。トレーニングマネージャは、「複数の[模擬フィッシング]テンプレートを使用することができ、包括的なレポート機能を提供するツールが必要であることは分かっていました」と述べています。

プログラムを開始する前に、サイバーセキュリティチームは、プログラムの開始が間近に迫っていること、プログラムの背景にある意図(Wombatが強く推奨するアプローチ及びトレーニングマネージャの独自の調査において反映されたアプローチ)について出資者と従業員全員に連絡しました。

「何よりも先ず、全ての出資者に確実に当社の計画を知ってもらうようにしました。人事チーム、ITヘルプデスクマネージャ、その他の主要メンバーとのミーティングを開始しました。良いパートナーであることが重要であることは分かっていました」とトレーニングマネージャは述べています。「初日からその原則に従いました。たとえば、ヘルプデスクの電話やメールを山積みにしたくないので、私たちは今でもITグループと連携して、シミュレートされた攻撃が、チームが多忙な週に予定されていないことを確認しています。」

しかし、次回の活動について手短に伝える相手は役員だけではありませんでした。トレーニングマネージャは「私たちは、これが人々にとって驚きとなることは望んでいませんでした。私たちは誰も不必要に混乱させたくありませんでした」。「エンドユーザからの苦情はたまにしかないというわけではありませんが、プログラムの背後で私たちが何をしているのか、「なぜ」そうしているのかをエンドユーザが理解できるように尽力することに役立っています」と述べています。

月1回の判定、上昇する難易度

公益事業会社は、ティーチャブル・モーメント(Teachable Moments)として知られる組み込み型のジャストインタイムのティーチングメッセージと組み合わされた、月1回のシミュレートされたフィッシング攻撃を決定しました。これらのメッセージは、エンドユーザが模擬フィッシュとやり取りするときにトリガされます。簡単な興味をそそるメッセージが、シミュレートされた攻撃の目的を説明し、将来のフィッシングメールを認識・回避するためのヒントを提供します。

＊Wombatは、全ての組織が、公益事業会社が実施したものと同様の月1回の“ThreatSimフィッシング判定スケジュール”を検討することを推奨しています。このアプローチにより、アドミニストレータは、異なるタイプのテンプレート、異なる脅威ベクトル(悪意のあるリンク、危険な添付ファイル、データ入力/識別情報のキャプチャ)、異なるメッセージスタイルをテストすることができます。ThreatSim内で利用可能な月1回のシミュレートされた攻撃とレポート機能により、組織は、経時的な傾向のより正確な状況を把握し、従業員が最も引っ掛かりやすい攻撃のタイプをより容易に特定することができます。

トレーニングチームがかなり早い段階で気付いた1つの傾向は、従業員が本質的に企業であるメッセージをクリックして返信する傾向がはるかに高いということでした。この傾向は、Wombatの2016 State of the Phish Reportの結果にも反映されていました。

「業務スタイルの模擬攻撃は常に、私たちが送信した他のメッセージよりも高いクリック率を有していました。私は、これは人々が従順であろうとし、当社にやってほしいと頼まれたことをやるからだと思います」とトレーニングマネージャは述べています。

トレーニングマネージャは、重要なトピックに対処するために難易度が上がったテンプレートを選ぶおよび/またはメッセージをカスタマイズする能力をアドミニストレータに与えることによって、プログラムが経時的に自然に進化することができる、WombatのThreatSim製品の柔軟性を利用しました。

日本コーネット・テクノロジー株式会社
CORNET TECHNOLOGY (TEL) 03-5817-3655 (代)
www.nihon-cornet.co.jp

Wombat Security Technologies（アメリカ、ピッツバーグ）は、世界的に有名なカーネギーメロン大学（CMU)の研究から生まれ、同大学のコンピューターサイエンス学部の教授陣によって設立されました。

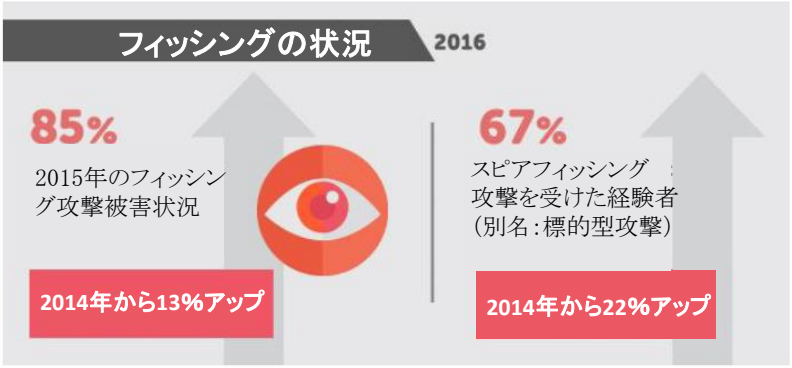
これらのタイプのシミュレートされた攻撃は、一部の従業員を落ち着かない気分にさせる場合がありますが、トレーニングマネージャは、出回っているビジネスメール詐欺攻撃の成功のレポートが、勝手に送り付けてくるメールを(それが「企業のように見える」通信であっても)額面通りに受け取るべきではないことをエンドユーザに理解させる必要性を高めることを知っています。

「本プログラムが成熟するにつれて、エンドユーザはこれらのタイプのフィッシュを見分けることがはるかにうまくなってきました」とトレーニングマネージャは述べています。

公益事業会社の数年にわたるプログラムが進行するにつれて、シミュレートされた攻撃の難易度がますます高くなっても、一貫した改善が見られています。トレーニングマネージャは、重要なトピックに対処するために難易度が上がったテンプレートを選び(又は)メッセージをカスタマイズする能力をアドミニストレータに与えることによって、プログラムが経時的に自然に進化することができる、WombatのThreatSim製品の柔軟性を利用しました。

「これまでは、文法の誤りや他のより『明白な』兆候を挿入することによって、それがフィッシュであることが人々に容易に分かるようにしていましたが、クリック率が下がるにつれて、私たちが送信しているキャンペーンの難易度を上げる努力をしました」とトレーニングマネージャは述べています

結果を確認するために、トレーニングマネージャは時折、月1回のローテーションの中に「より簡単な」シミュレートされた攻撃を入れています。「最近は、プログラムの初期段階であれば受け取る人が多数いたに違いないと思われるメールを送信しました」とトレーニングマネージャは述べています。「しかし、この段階では、クリックスルーは殆どありませんでした」



的を絞った季節的な判定

公益事業会社のトレーニングチームは、長い間、シミュレートされた攻撃を開発する際に現実主義を取り入れる必要性を強調してきましたが、実際に被害が出ている攻撃に目を光らせており、時間的制約のある季節的なシミュレートされたフィッシングメールを、現実の攻撃者が採用するアプローチを模倣するためのラインナップに含めています。トレーニングチームは、このことは、従業員に職場や個人的な通信においてよく見かける可能性が高い脅威を認識し、それに対応する準備をさせるのに役立つと感じています。

また、組織はThreatSimのシミュレートされた攻撃を使用して、的を絞ったトレーニングを行っています。
「自社の業種の一部であると感じられるメールの配信を試みるために、会議の登録やその他の業界固有のイベントおよびトピックを中心としたキャンペーンを行いました」とトレーニングマネージャは述べています。
「異なるトピックは異なるビジネスの分野の共感を呼ぶので、それらのメッセージのカスタマイズを可能にするのに役立ちます」

WombatのThreatSim製品内で利用可能なカスタマイズオプションは、サイバーセキュリティチームが開発したシミュレートされたビジネスメール詐欺攻撃において特に有用でした。いくつかの不正な電信送金詐欺メッセージが公益事業会社の企業メールフィルタを通過した後、トレーニングマネージャは、社内の役員および上層部マネージャを対象とした内部**ホエーリングキャンペーン***を行うことを決定しました。

公益事業会社の従業員の大半はフィッシング攻撃を見分けるのに成功していましたが、トレーニングマネージャは、**組織が依然として高度な的を絞ったスピアフィッシング攻撃を受けやすい**場合があることを心配していました。

＊ホエーリングキャンペーン
「フィッシングの一種で、CEO(最高経営責任者)やCFO(最高財務責任者)などの経営層になりすまし、社員に対して偽のメールを送るもの」

「役員の各々に対してシミュレートされたフィッシングメッセージをカスタマイズしました。当社のチームはLinkedInに登録し、Googleを使用して、そこに出回っている容易に入手可能な情報、幹部が所属している組織やプログラムなどの詳細を見つけました」とトレーニングマネージャは述べています。

トレーニングマネージャによれば、このキャンペーンは非常にインパクトの強いものでした。
「私たちは、受信者の不意を突きたくなかったので、的を絞ったキャンペーンを行う予定であることを事前に受信者に通知しました。そうしたにもかかわらず、メッセージが説得力のあるものだったので、クリック率はかなり高くなりました」

カスタマイズされたシミュレートされたホエーリングキャンペーンは、「[公益事業会社の]役員が得る貴重な教訓と、役員がその教訓を得るのに非常に効果的な方法」を与えました。

日本コーネット・テクノロジー株式会社
(TEL) 03-5817-3655 (代)
www.nihon-cornet.co.jp

カーネギーメロン大学での研究から誕生した「企業や組織のサイバーセキュリティに対する認識や意識を変え，他に類を見ない低コストでリスクを減らす包括的なセキュリティトレーニングソリューション」

この演習は、どのようにすればThreatSimのシミュレートされた攻撃をカスタマイズし、的を絞ったものにすることができるか、それらの攻撃がどれだけソーシャルエンジニアリングの現実を理解させることができるかの好例でした。また、この演習は、やりがいのある課題を提供し、フィッシングメッセージがどのようなものなのかについてのエンドユーザの理解を継続的に深めたいというトレーニングマネージャの願望を強固なものにしました。結局のところ、攻撃者、特に特定の人々やシステムにアクセスしようとしている攻撃者は、頻繁にソーシャルメディアを頼りにし、信頼できるように見える詳細を使用して、疑うことを知らない受信者をだまします。

「私たちは、攻撃者が毎日考え、行動しているやり方で、考え、行動しました」とトレーニングマネージャは述べています。**「これは、当社の役員が得た貴重な教訓であり、役員がその教訓を得るのに非常に効果的な方法でした」**

- **トレーニングの実施及び保持を改善するための強化**

フィッシング判定に加えて、サイバーセキュリティチームは、教育・強化技法をセキュリティ・アウェアネス及びトレーニングプログラムに組み込んでいます。Wombatの継続的トレーニング方法の基本要素であるこれらのコンポーネントは、知識の保持を改善し、1年を通じてベストプラクティスを念頭に置くのに役立ちます。

シミュレートされたフィッシング演習に加えて、教育コンポーネントを含めるようにプログラムを拡大することに課題がなかったというわけではありません。「経営陣は組織にさらなる負担をかけたくなかったので、トレーニングを承認してもらうことも困難でした」とトレーニングマネージャは述べています。「しかし、最終的には、経営陣は、サイバーセキュリティトレーニングがいかに重要であるかを認識しました」

主なサイバーセキュリティメッセージを強化するために、チームは共用エリアにポスターを貼り、同社のウェブサイトのあるセクションを、フィッシングやメールセキュリティのベストプラクティスについての情報の提供に充てています。
また、チームは、WombatのPhishAlarm®メールレポートボタンを自社のメールクライアントに組み込んでいます。このツールは、従業員がマウスを1回クリックするだけで疑わしいメッセージを組織のセキュリティ対応チームにレポートすることを可能にし、脅威の検出および防止に積極的に参加する機会をエンドユーザに与えます。

「PhishAlarmボタンについては非常に良いフィードバックを得ています」とトレーニングマネージャは述べています。
「ユーザはPhishAlarmボタンを本当に気に入っています」

これらのタイプのツールを使用することに加えて、サイバーセキュリティは、セキュリティ・アウェアネスの文化を構築しようとして、従業員基盤と継続的に関わっています。1年間の通信カレンダーが事前に作成され、サイバーセキュリティ・アウェアネスのトピックが1年を通じて提供されます。そのうえ、公益事業会社がアクティブなフィッシング攻撃を受けている場合、チームはメールを介して警報を送信します。

しかし、おそらく最も印象深いのは、この組織のセキュリティ賛同者プログラムです。このプログラムは、700名以上のメンバーを擁しており、情報を広め、会話ポイントを作るための効果的な手段を提供しています。サイバーセキュリティチームは賛同者と定期的に交流しており、賛同者はチームや賛同者仲間と話をしています。このアプローチは、組織的にセキュリティイニシアチブの範囲を広げ、主なセキュリティメッセージの局所化と対象設定を可能にします。

- **目に見える結果**

公益事業会社のセキュリティアウェアネス・トレーニングプログラムの成功は、より積極的に関与している従業員の事例証拠をはるかに超えるものです。ThreatSimの広範なレポート機能と公益事業会社独自のパフォーマンス測定により、組織は、月1回のシミュレートされた攻撃キャンペーンとフィッシングアウェアネスに関するメトリックを正確に追跡することが可能になりました。その結果として、著しい進歩がみられています。

- **クリックレートとフィッシング感受性の低下**

2013年6月当時、公益事業会社のベースラインキャンペーンでは、クリックレートは32%でした。
2015年末現在、年初来平均は10.42%でした。このクリックレートの21.58%の改善は、67.43%の感受性の低減に相当します。

トレーニングマネージャは、「～ライクな」シミュレーションに関する前年比の改善を測定できるようになったことも指摘しています。「前に述べたように、世間に出回っているパターンを利用するために、本質的に季節的なものであるメッセージを送信したいと思っています。このため、連続3年間にわたって12月に、いくつかのバリエーションがあるシミュレートされた出荷通知メールを送信しました」とトレーニングマネージャは述べています。
「それらの3つの攻撃に関連するクリックレートは22%→15%→7%となりました。これは、ユーザが確実に学習していること、注意を払っていること、今では開始したときよりも良い判断を下していることを示しています」

ビジネスパートナー（一部）

IBM Security / CAMBRIDGE EDUCATION THE POWER OF KNOWLEDGE / TELSTRA / KASPERSKY lab / bsi. / RSA / ISO 9001 : 2008 REGISTERED FIRM Capgemini CONSULTING.TECHNOLOGY.OUTSOURCING / dimension data / Future Com / Secure Link / CRITICALSTART

CDM / INFOSEC AWARD WINNERS ★ 2017 ★

日本コーネット・テクノロジー株式会社
CORNET TECHNOLOGY (TEL) 03-5817-3655 (代)
www.nihon-cornet.co.jp

GARTNER'S MAGIC QUADRANT

wombat security technologies

Wombat Security Technologies社のセキュリティ・アウェアネス（認識）及びトレーニングソリューションは、3年連続して Gartner Magic Quadrant for Security Awareness Computer-Based Training Vendors のリーダーとなっています。

改善されたセキュアな挙動メトリック

公益事業会社は、基本的な技術的対策/サイバーセキュリティ対策に関する従業員の挙動と意思決定プロセスを評価する年1回の企業セキュリティ判定に参加しています。調査票は、シニアマネージャから個々の貢献者まで、企業のすべての役割と責任を対象として送付されます。合計で2,000人以上の人々が評価に参加しています。ユーザは、機密情報のコピーを取る、機密情報をメールする、パスワードを共有するおよび/またはパスワードを書き留める、機密資料を無防備なままにする、デスクから離れるときにコンピュータシステムをロックするのを忘れる、などの行為について判定されます。

2016年のPhish Reportデータでは、Wombatのフィッシング対策トレーニング後、クリック率が平均で

64%

改善されています。

これらのポリシー関連の「はい/いいえ」のインジケータに加えて、従業員は、フィッシングメールをクリックするといったリスクを伴う挙動を回避する能力について評価されます。
調査票には、添付ファイルを開く傾向や非ビジネス関連のメールのリンクをクリックする傾向など、組織に対するリスクの認識に関する質問が含まれています。
（フィッシング対策プログラムの開始前であった)2012年の全社的な判定では、「フィッシングを回避する」セキュアな挙動メトリックは91%でした。
2015年の判定では、意思決定プロセスの大幅な改善が反映され、同じ挙動メトリックに対して99%を示しました。

経営トップからの称賛と感謝

このプログラムとその成功は、組織の一部の最上層部で認められ、話題になっていました。
「一連の最近のリーダーシップトレーニングイベントにおいて、当社の社長がフィッシングプログラムを絶賛していました」とトレーニングマネージャは述べています。
「一部の会議では1,000人以上の人々が出席し、社長は私たちの努力がもたらす影響と重要性を強調していました」

「経営陣からのこのレベルのサポートは、本当に正当性が認められているということです。多くの情報セキュリティチームではそのようなサポートを得られないということを直接耳にしているので、私たちは幸運だと思います」とトレーニングマネージャは述べています。「私たちがサポートを得られていることを非常に嬉しく思います。これは、トップダウンの支援は本当に効果があり、私たちの成功に役立ったからであると思います」

将来に目を向ける

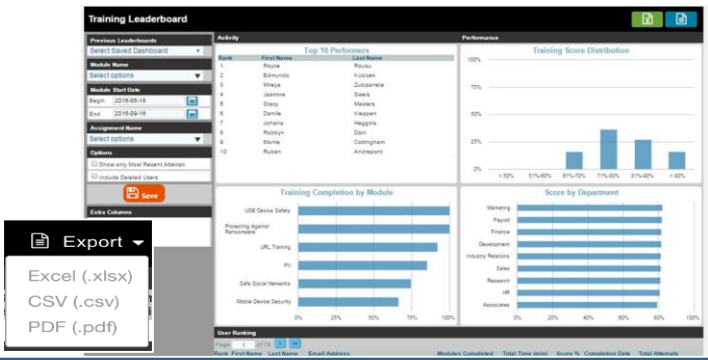
公益事業会社では、月1回のフィッシング判定を減らす予定はなく、トレーニングマネージャは、さらにいっそう独創的にし、エンドユーザに対する課題のレベルを上げるつもりであると述べています。

「ニュースでフィッシング攻撃をよく見ることが助けになっています」とトレーニングマネージャは述べています。「一方では、これらのフィッシング攻撃が依然として発生していることは良くないことですが、他方では、そのことがこの手のアウェアネス及びトレーニングプログラムの必要性を証明し続けています」

更に、トレーニングマネージャは、シミュレートされたフィッシングを組み込むことを躊躇している組織に再検討するよう働き掛けています。「『自社の従業員をだましたくない』と言う組織があることを知っています。このため、こうした組織は、シミュレートされた攻撃を行うことを敬遠しています。しかし、当社の役員は全員、すべての技術制御の中で最も簡単で最も速い方法は人間であるということを理解しています」とトレーニングマネージャは述べています。

トレーニングマネージャは改めて、役員の支援の価値を強調しています。「当社のリーダーたちは、サイバーセキュリティチームとこのプログラムを本当にサポートしてくれています。また、これには従業員も共感しています。従業員は、上層部から聞いたことは真剣に受け止める必要があるということがわかっているからです」

「当社の幹部は、すべての技術制御の中で最も簡単で最も速い方法は人間であるということを理解しています」



日本コーネット・テクノロジー株式会社
CORNET TECHNOLOGY (TEL) 03-5817-3655 (代)
www.nihon-cornet.co.jp