Webster Bank

お客様が影響を受ける前にオンライン詐欺を食い止める

概要

ニーズ

Webster Bank は、銀行のセキュリティー・プログラムを拡張して、同行の Web-Link オンライン・バンキング・プラットフォーム上で詐欺に遭わないように法人顧客をプロアクティブに保護する必要がありました。

解決策

Webster Bank は、IBM の Trusteer™ ソフトウェアを基にした、エンドポイントを中心とした詐欺防止ソリューションを導入して、マルウェア感染およびフィッシング攻撃からモバイル・デバイスおよびデスクトップ・デバイスを保護できるようにしました。

利点

12 カ月間で 224 の感染が検出および解決され、詐欺により数百万ドルの損失が出る可能性を回避できました。

Webster Bank は 210 億米ドル (1 ドル 100 円換算で約 2 兆 1,000 億円) の資産を有し、南ニューイングランド地方およびニューヨーク州ウエストチェスター郡一帯の企業、政府機関、非営利団体、および個人に、銀行取引、資金管理、住宅ローン、民間銀行、信託、投資サービスを提供しています。

マルウェア感染およびフィッシング攻撃から顧客を保護

もし金融詐欺を発生前に食い止めることができたらどうだろう。 それが、2011 年に Webster Bank が持った疑問でした。同行は、電信送金や電子小切手決済 (ACH) で発生した異常にフラグを立てる先進的なリスク・エンジンを始めとする、多くのセキュリティー層をすでに装備していました。

Web-Link オンライン・バンキング担当の VP 兼シニア・プロダクト・マネージャーの Kim Swart 氏にとって、顧客が新しいソリューションを素早くインストールできることが不可欠でした。「ベンダーはよく「速くて簡単です」と言いますが、実際にはそうでもないことが多いのです。しかし、Trusteer を個人用のデバイスやコンピューターにダウンロードした際、インストールに 60 秒もかからなかったのを見たのは、私たちにとってうれしい驚きでした」と Swart 氏は述べています。

ソリューション・コンポーネント

ソフトウェア
- IBM® Security Trusteer Rapport™
- IBM Security Trusteer™ Mobile App (セキュア・ブラウザー)

これらの方法は極めて効果的で、不正取引が発生するとすぐに発見し、すぐに処置できていたのですが、同行では、最初から不正取引が発生するのを食い止めることができるセキュリティー層の追加を考えるようになりました。

Webster Bank の最高情報セキュリティー責任者の Jack Stoddard 氏は次のように説明しています。「世の中には無数のマルウェアが存在します。弊社には詐欺を追跡調査する非常に優れたプロセスがありましたが、その状態ではいやだったのです。詐欺そのものを締め出してしまいたかったのです。」

同行の Web-Link オンライン・バンキング担当 VP シニア・プロダクト・マネージャーの Kim Swart 氏も同様に次のように述べています。「最適な保護を提供すると同時に、お客様にとってできる限りシームレスなプロセスがほしいと考えていました。 ハードウェア・トークンを持ち運びたくないという要望を、お客様ははっきりと私たちに伝えておられました。」

リスクおよび顧客への影響を最小限に抑える

いくつかの製品を検討した後、同行のセキュリティーおよび業務の担当者は、IBM が提供する、エンドポイントを中心とした詐欺防止ソリューションである TrusteerRapport™ ソフトウェアを選択しました。

Stoddard 氏は次のように述べています。「Trusteer Rapport を使用すると、お客様は作業の中断を最小限に抑えて最大の効果を得られます。このソフトウェアは素早くダウンロードでき、インストール後はバックグラウンドで作動してフィッシング攻撃およびマルウェア感染からお客様を保護します。」

Webster Bank の Web-Link の顧客は、Trusteer ソフトウェアをオンライン・デバイス上にダウンロードします。このソフトウェアは、フィッシング攻撃を阻止し、犯罪者が企業アカウントを乗っ取り、資金を盗むのを可能にするマン・イン・ザ・ブラウザー・マルウェア株がインストール・稼働するのを防ぎます。Trusteer ソフトウェアは現在世界中でアクティブなフィッシングやマルウェアの攻撃に関する情報を収集し、行動アルゴリズムを適用して、命名済みの脅威および潜在的な新しい脅威の両方を阻止します。

「Trusteer ソフトウェアのインストールを必須にして以来、弊社ではオンライン詐欺にまで発展した感染の例はありません。」

—Jack Stoddard 氏 (Webster Bank 最高情報セキュリティー責任者)

このハイレベルの保護と顧客への影響を低く抑えるという組み合わせは、Webster Bank にとって正しい選択となりました。Webster のスタッフは次々に各顧客セグメントと連携し、このソフトウェアがスムーズに各グループで採用できるように注意を払い、適切なサポートを提供しました。

モバイル・ブラウザーの導入

Web-Link の顧客による Trusteer Rapport ソフトウェアの導入の義務付けを計画し始めた頃、Webster のスタッフはデスクトップとラップトップにのみ焦点を合わせても不十分であることに気が付きました。

「法人のお客様用のモバイル・アプリケーションはまだ作成していませんでしたが、一部のお客様が弊社のサイトにアクセスするためにモバイル・デバイスを使用していることに気が付きました。
と Stoddard 氏は述べています。「モバイルは、ハッカーが次に目をつける分野であるため、備えておきたいと考えました。」

この問題に対応するために、チームは Trusteer Mobile App (セキュア・ブラウザー) も実装して、顧客がモバイル・デバイスから Web-Link に安全にアクセスできるようにすることにしました。

「Trusteer Mobile App は簡単に実装でき、モバイル・デバイスから弊社のサイトへのアクセスを保護するという問題をすぐに解決してくれました。今、Web-Link オンライン・バンキング・プラットフォームをアップグレードし、カスタム・モバイル・アプリケーションを構築するにあたり、弊社では、Trusteer と連携して、Trusteer Mobile SDK [software development kit] を実装する予定です」と Swart 氏は述べています。

顧客による 100 % の採用を目指す

プログラムの立ち上げ後 4 カ月以内に、約 30% の Webster Bank の法人顧客がこの新しい詐欺防止ソリューションをダウンロードしました。この時点では、プログラムへの参加は任意でした。

「詐欺が至るところで多発しているため、お客様は Trusteer によって高度に保護された環境でのバンキングが可能になった考えておられます。」

—Kim Swart 氏 (Webster Bank Web-Link オンライン・バンキング担当 VP 兼シニア・プロダクト・マネージャー)

しかし、詐欺件数ゼロの目標を達成するには、このソフトウェアの完全な採用が必要であること、つまり、プログラムを必須にする必要があることをチームは認識していました。 そのためには、情報技術、預金業務、顧客サービス、実装の各分野から集めた人材と、財務および決済ソリューション、商業銀行業務、政府銀行業務、および企業金融業務などのビジネス分野の人材をまとめ、チームとして連携させる必要もありました。 この必須採用の実施に向けた職能上の枠を超えたアプローチが成功の鍵となりました。

この取り組みの一環として、チームは、プログラムを必須にするほぼ 9 カ月前に包括的な教育計画の立ち上げを開始しました。

「関係チームが Trusteer の利点をお客様に伝えることができるように、まず関係チームにその利点を伝えるのに多くの時間を使いました」と Swart 氏は述べています。

顧客のソフトウェアの採用を促進するために、チームはスプラッシュ・ページの表示頻度も 3 日に 1 回から 1 日 1 回に増やしました。「スプラッシュ・ページの頻度を上げると、お客様からご意見をいただけるようになりました。新規のお客様ごとに詐欺チェックリストも提供し、Trusteer Rapport もその話し合いの一部として含めています。」

Swart 氏はさらに続けます。「この教育は成功しました。Rapport を任意ダウンロードとして提供し始めたとき、ダウンロードを強制された場合は取引を停止するというお客様が少数おられました。私たちは、このような抵抗を乗り切る方法について関係チームと戦略を練りました。そしてこの教育の取り組みを通じて、Rapport を必須にするにあたり、Web-Link を介してオンライン決済を行うすべての顧客が Trusteer を使用することを必須とすることに成功したのです。」

数百万ドルにのぼる詐欺の可能性を回避

必須となったこの Trusteer 詐欺防止プロジェクトは、9 カ月間の採用期間中に採算が取れました。また、ソフトウェアを実装してから最初の 12 カ月間で、224 の感染が検出および解決され、詐欺により数百万ドルの損失が出る可能性を回避できました。

「これらのマルウェア感染は、通常、実際に詐欺被害に遭う第一歩となります。Trusteer ソフトウェアのインストールを必須にして以来、弊社ではオンライン詐欺にまで発展した感染の例はありません」と Stoddard 氏は述べています。

このように保護の水準を高めることで、詐欺に対するセキュリティーへの顧客の信頼が高まりました。

Swart 氏は言います。「詐欺が至るところで多発しているため、お客様は Trusteer によって高度に保護された環境でのバンキングが可能になったと考えておられます。あるケースでは、お客様から保護についてお礼の E メールまでいただきました。Web-Link のお客様とお話すると、このソフトウェアがお客様の Webster Bank との通信を保護するのに役立つだけでなく、他の金融関連の Web サイトでもお客様を保護するのに役立つという追加の価値があることにお客様は気付かれています。」

詳細情報

IBM Security Trusteer ソリューションについて詳しくは、IBM 営業担当員または IBM ビジネス・パートナーにお問い合わせいただくか、次の Web サイトをご覧ください。 **ibm.com**/security

Webster Bank について詳しくは、次の Web サイトをご覧ください。
http://www.websterbank.com

日本 IBM 株式会社
東京都中央区日本橋箱崎町 19 番 21 号

Produced in Japan
August 2014

本書の情報は最初の発行日の時点で得られるものであり、予告なしに変更される場合があります。 すべての製品が、IBM が営業を行っているすべての国において利用可能なのではありません。

記載されている性能データとお客様事例は、例として示す目的でのみ提供されています。実際の結果は特定の構成や稼働条件によって異なります。IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

本書に掲載されている情報は特定物として現存するままの状態で提供され、第三者の権利の不侵害の保証、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されています。IBM 製品は、IBM 所定の契約書の条項に基づき保証されます。

お客様は自己の責任で関連法規を遵守しなければならないものとします。IBM は法律上の助言を提供することはいたしません。また、IBM のサービスまたは製品が、お客様がいかなる法規も遵守されていることの裏付けとなると表明するものでも、保証するものでもありません。

適切なセキュリティーの実施について: IT システム・セキュリティーには、企業内外からの不正アクセスの防止、検出、および対応によって、システムや情報を保護することが求められます。不正アクセスにより、情報の改ざん、破壊もしくは悪用を招くおそれがあり、またはシステムの損傷や、他のシステムへの攻撃を含む悪用につながるおそれがあります。完全に安全と見なすことができる IT システムまたは IT 製品は存在せず、 また単一の製品またはセキュリティー対策が、不正アクセスを防止する上で、 完全に有効となることもありません。 IBM のシステムおよび製品は、包括的なセキュリティーの取り組みの一部となるように設計されており、 これらには必ず追加の運用手順が伴います。また、最高の効果を得るために、他のシステム、製品、またはサービスを必要とする場合があります。IBM は、何者かの悪意のある行為または違法行為によって、システムおよび製品が影響を受けないことを保証するものではありません。


Please Recycle

WGC12362-JPJA-00