Pulaski Bank

先進的な不正防止ソリューションで小売店および商業企業の顧客をサイバー犯罪から守る

スマートとは、

顧客が影響を受ける前に潜在的な不正を防ぐこと

金融業界全体では、銀行でオンライン不正の発生を検知・対応するための強力なセキュリティー対策を実装する処置がすでに講じられています。Pulaski Bank では、これに加えて、発生する前に不正を防止するための対策が講じられています。ユーザーのログイン時の不審な挙動を検知する IBM の高度な不正防止ソリューションの導入により、同銀行ではマルウェアに感染したデバイスを素早く特定し、潜在的な不正を予防するための対応策を取ることができます。

Pulaski Financial Corp. の傘下にある Pulaski Bank は、セントルイス市街にあるフルサービスを提供する 13 の支店を介して、小売店および商業企業向けのバンキング・プロダクトをすべて取り揃えて提供しています。 また同行では、セントルイス市街、カンサスシティー市街、シカゴ市街、ミズーリ中部、ミズーリ南西部、カンサス東部、オマハ (ネブラスカ)、カウンシルブラフス (アイオワ) で展開するローン・プロダクション・オフィスを介して住宅ローン製品も提供しています。

2012 年、Pulaski Bank のマネジメント・チームは同行のオンライン・バンキング・プラットフォームの更新に取り掛かりました。

銀行業務担当シニア・バイス・プレジデント、Denise DeRousse によると、同行は、その小売店および商業企業の顧客に「地域密着型の銀行という印象」を与える、競争力のある金融製品を提供するために、「最高級の」プラットフォームを構築することを目指しました。

チームの計画が進むにつれ、セキュリティーが重要な因子になってきました。

「私たちにとってセキュリティーは、企業やサービスの成長と並ぶ最重要事項です。そのため、プラットフォームに関しても「群を抜いて優れたもの」を提供したかったのです」と DeRousse は述べています。

確かに、サイバー犯罪者がマルウェア攻撃やフィッシング攻撃によって顧客の口座を乗っ取ったり、不正な取引を行ったりするため、今日すべての銀行にとって、不正防止は依然として主要な関心事項です。

ビジネス利益

- 不正防止: ひと月に 72 個の感染を検出・解決して、顧客の取引を保護し、潜在的な損失を防ぎました。
- コンプライアンス: 同行の米国連邦金融機関検査協議会 (FFIEC) の新しいガイドラインへの遵守を支援しました。
- カスタマー・エクスペリエンス: プロアクティブなコミュニケーションによって顧客との関係を強化しました。

Pulaski Bank はすでに多数の不正予防手法を実装していました。 例えば、小売業の顧客向けのオンライン支払いサービスにおける異常を検知し、スタッフに知らせる高度なツールを採用していました。 また、同行の商用オンライン・バンキング・サービスには、多要素認証、およびログインごとにワンタイム・パスワードを生成する VASCO トークンが導入されていました。

しかし、同行では、セキュリティー層が多ければ多いほど、顧客をよりよく保護できることを理解していました。 資金管理および電子バンキング担当 VP、Suzy Morris によると、このことは、米国連邦金融機関検査協議会 (FFIEC) の新しいガイドラインでも確認されています。

顧客エンドポイントへのマルウェア攻撃およびフィッシング攻撃の検知と阻止

同行では、顧客のエンドポイント上のマルウェアを検知し、解決する不正防止ソリューションの候補が 3 つ選ばれました。 これらの製品を検討中に、デプロイメントと保守が容易で、顧客が容易に使えるソリューションの探求が行われました。

「私たちは、お客様側に何かすることをお願いすることなしに、潜在的な問題を特定し、必要に応じてお客様に手を差し伸べるやり方を希望していました」と Pulaski Bank の情報システム担当 VP の Tom Modde が述べています。 「また、お客様 1 人あたりの価格やインストールおよび管理にかかるコストについても考慮しました。その結果、IBM の Trusteer ソフトウェアがトップになりました。また、このソフトウェアが提供する価値が最も大きいことが判明し、さらに弊社の既存のプラットフォームとの統合も容易であると思われました。」

よりスマートなバンキング: 不正をその場で阻止する

機能化

この不正防止ソリューションでは、ユーザーが銀行のネットワークにアクセスするたびに、スキャンによって潜在的な脅威の存在の確認を行います。

相互接続

このソフトウェアは、世界中に散在する 270,000,000 個以上のエンドポイントをモニターして、アクティブなマルウェア攻撃やフィッシング攻撃に関する情報を収集し、取り込みます。

インテリジェント化

行動アルゴリズムを使って、新しい異形を含むマルウェアを検知、阻止、削除し、ゼロデイ脅威に対応します。

Let's build a smarter planet

ソリューション・
コンポーネント

ソフトウェア

- IBM® Security Trusteer Pinpoint Malware Detection™ Advanced Edition
- IBM Security Trusteer Rapport™

「私たちにとってセキュリティーは、企業やサービスの成長と並ぶ最重要事項です。そのため、プラットフォームに関しても「群を抜いて優れたもの」を提供したかったのです。」

—Denise DeRousse (Pulaski Bank、銀行業務担当シニア・バイス・プレジデント)

優れたカスタマー・サービスのためのプロアクティブなアプローチ

現在、IBM® Security Trusteer Pinpoint Malware Detection™ Advanced Edition は Pulaski Bank のオンライン・バンキング・プラットフォームと統合されています。これにより、マルウェアに感染したデバイスやマルウェア攻撃のクライアントレス検知が可能になりました。同行の顧客がオンライン・バンキング・プラットフォームにアクセスすると、ソフトウェアはユーザーのデバイスを分析して感染していないかを確かめます。マルウェアを検知すると、ソフトウェアは自動的に銀行のコール・センター・チームに警報を出します。

「弊社のコール・センター・チームに脅威警報を提供することで、私たちはお客様に必要な技術的なサポートを提供できるだけでなく、コール中に発生するかもしれないその他の質問に答えることもできます」と Morris は述べています。「この触れ合い型のアプローチは、弊社のカスタマー・サービスのスタッフが既に実行して非常に成果を上げている方法の延長上にあることがわかりました。」

カスタマー・サービスのスタッフは、IBM Security Trusteer Rapport™ ソフトウェアを使用してユーザーが問題を解決するのを支援します。このソフトウェアは、Trusteer Pinpoint™ ソフトウェアと同様、IBM が提供するクラウド・ベースのサービスを使ってデプロイされます。Trusteer Rapport ソフトウェアの顧客のデバイスへのインストールにより、マルウェアは削除され、デバイスは将来の感染からも保護されるため、ユーザーは安全に自分のマシンからオンライン・トランザクションを実行することができます。

「弊社はお客様側に何かするよう要求することをしたくなかったため、Trusteer Pinpoint Malware Detection を弊社のオンライン・バンキング・プラットフォームに実装しました」と Morris の説明は続きます。「また、希望されるお客様だけに修復用の Trusteer Rapport のダウンロードを提案したり、ビジネスをオンラインで行うお客様のデバイスをよりセキュアにするための支援を提供したりしています。」

スタッフ効率の最大化

地方銀行の社員にはいろいろな仕事をこなすことが要求されます。そのため、どのような新しいテクノロジーであっても、その導入により社員の仕事が煩雑になることがなく、より働きやすくなることが最優先です。Morris によると、IBM の Trusteer™ ソフトウェアはこの要件をしっかり満たし、チームがより容易にチームの目標を満たすことを可能にしました。

「弊社では通常 1 日に 2 つから 5 つのアラートが発生しており、このソリューションの使用法が非常に簡単であるため、これらのアラートへの対応はコール・センター・チームの活動に組み込まれています」と Morris は述べています。

「弊社では通常 1 日に 2 つから 5 つのアラートが発生しており、このソリューションの使用方法が非常に簡単であるため、これらのアラートへの対応はコール・センター・チームの活動に組み込まれています。」

– Suzy Morris (Pulaski Bank、資金管理および電子バンキング担当 VP)

銀行のスタッフにはまた、感染しているデバイス、感染時期、および悪意のあるエクスプロイトの名前が表示された、包括的で、見やすいレポートが届けられます。

「これらのレポートによって、市場で起きていることを把握して、ニュースでそのことが報道される前に対処することができます」と Morris は述べています。

この情報はまた、コンプライアンス・イニシアチブのサポートにも用いられます。

「弊社ではこのソフトウェアを使用して FFIEC の規制要件をクリアし、このレポートを使用して監査員にコンプライアンスを実証しています」と DeRousse は付け加えています。

守りを固めて不正による損失を防ぐ

Morris にとって、このプログラムの成功を示す 1 つの指標に、脅威から身を守るために Trusteer Rapport ソフトウェアを自主的にダウンロードすることを選択した小売店および商業企業の顧客数の多さがありました。その数は 18 カ月という短期間に 10,831 社に上りました。

「弊社のセキュリティー措置に対するお客様の反応は好意的で、自分のアカウントへの不正アクセスが発生する前に脅威を解決するための支援を提供したことに対して感謝していただいています」と Morris は続けています。 「お客様からは、弊社が多様な分野で素晴らしいサービスを提供しているという話をきいています。このプログラムもその「優れたサービス」の 1 つであると思っています。」

また、IBM の不正防止ソリューションの使用により、先月だけで約 72 個の感染が検知・解決されました。 「このソリューションによって、弊社は潜在的な不正を防ぐと同時に、お客様の認識を高めることもできました」と Modde は言っています。

好意的なフィードバックと保護の強化を手に入れた Pulaski Bank は、現在このプログラムをモバイル顧客まで拡張することを計画しています。

「私たちは、Trusteer Mobile SDK と弊社のモバイル・バンキング・プラットフォームの統合についてオンライン・バンキング・プロバイダーと相談しています」と Modde は述べています。

「このソリューションによって、弊社は潜在的な不正を防ぐと同時に、お客様の認識を高めることもできました。」

– Tom Modde (Pulaski Bank、情報システム担当バイス・プレジデント)

裏話: 目標への確実な道作り

Morris によると、社内での社員向けの教育、および社外での顧客向けの教育の両方がこのプログラムの成功に欠かせませんでした。 教育は、カスタマイズしたスプラッシュ・ページ、オンライン広告、収支報告書を送付する封筒に同封した広告、e-バンキングのセミナーを利用して行われました。

「弊社のオンライン・チャネルを利用して、私たちはお客様と対応するすべての社員に確実にこの不正防止ソリューションについての知識を持たせるようにしました」と Morris は述べています。 「また、一連の教育イニシアチブを立ち上げて、弊社のオンライン・バンキングのお客様が自分たちが直面する脅威を理解し、さらに Pulaski Bank がお客様のリスク軽減のお手伝いをしていることを知っていただけるようにしました。 私たちは、リスクおよび弊社の取り組みに関するセミナーやその他の支援活動を提供することは、将来大きな価値を生み出すと考えています。」

詳細情報

IBM がどのようにお客様のビジネスの変革を支援できるかの詳細については、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、**ibm.com**/security をご覧ください。

Pulaski Bank の詳細については、www.pulaskibank.com/ をご覧ください。

Let's build a smarter planet

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

WGC12365-USEN-00