IBM Security

金融サービス・セクターにおけるセキュリティーのトレンド

お金もデータも狙われ、2016 年の攻撃標的が引き続きサイバー犯罪の対象となる

IBM X-Force® リサーチ

2017 年 4 月発行

IBM

目次

要旨

金融サービス・セクターは、ここ 20 年以上、サイバー犯罪対象の中心となっており、2016 年もまた同様でした。2017 年の「IBM X-Force Threat Intelligence Index」で明らかにされたように、このセクターが他のどの業界よりも多く攻撃を受けました。IBM Security Services がモニターした金融サービスの平均クライアント組織は、全業界での平均クライアント組織より 65 % 多くの攻撃を受けました (図 1 を参照)。さらに、2016 年には、金融サービスの組織で攻撃が平均 29 % 増加し、2015 年[1] には 1,310 件であった攻撃が、2016 年には 1,684 件に増えています。

しかし、こうした負の調査結果がある中で、良い知らせもあります。金融サービスのモニターした平均クライアントで、2015 年[2] には 192 件であったセキュリティー・インシデントが、2016 年には 94 件に留まりました。「セキュリティー・インシデント」は、最も重大な区分であるため、これは歓迎すべきニュースです。

用語の定義

セキュリティー・イベント: セキュリティーのデバイスまたはアプリケーションが検出した、システムまたはネットワーク上のアクティビティー。

攻撃: 情報システム・リソースまたはその情報自体を収集、中断、拒否、低下、破壊しようとしている悪意のあるアクティビティーであると、相関・分析ツールが識別したセキュリティー・イベント。

セキュリティー・インシデント: IBM セキュリティー・アナリストが検討し、さらに調査すべきと判断した攻撃またはセキュリティー・イベント。

図 1. IBM Security Services がモニターした平均クライアント組織に関する 2016 年の全業界と金融サービスの比較。(セキュリティー・イベント、攻撃、セキュリティー・インシデントの定義については、横枠の「用語の定義」を参照してください。)

IBM Security

残念ながら、良いニュースはこれで終わりかもしれません。
IBM® の世界的なセキュリティー研究機関である X-Force® でサイバー犯罪行為のトレンドと金融マルウェアの動きを調査しているマルウェア・リサーチャーによって、2016 年に一部の国で金融のサイバー犯罪行為が著しく増加していることが分かりました。サイバー・ギャングは、2014 年半ばで加速し始めたトレンドとして、Dyre、Dridex、GozNym、TrickBot などのマルウェアを使用してビジネス・バンキング・サービスをターゲットとし、ビジネス・バンク・アカウントに焦点を合わせています。

また、2016 年には、何千もの銀行や企業が世界中で送金に使用するメッセージング・システムに対する、公的に報告された Society for Worldwide Interbank Financial Telecommunication (SWIFT) 攻撃が、顕著に増えています。[3]
その結果、カスタム・マルウェアを使用してさまざまなグローバル・バンクから何百万米ドルもが盗まれて不正に送金され、こうした取引の痕跡が消されました。

このレポートで示された他の分析と合わせ、こうしたトレンドやインシデントは、金融サービス・セクターの困難な実態を表しています。幸い、金融サービス組織は、内部者の脅威や金融マルウェアといったセキュリティー上の大きな痛点の緩和にフォーカスして、サイバー・セキュリティーの免疫システムを強化することができます。

このレポートについて

この IBM X-Force リサーチのレポートは、IBM Managed Security Services の Threat Research グループによって作成されました。このグループは、IBM のお客様に情報を提供し、最新のサイバー・セキュリティーの脅威に対して準備できるように日夜取り組んでいる経験豊かな熟達したセキュリティー分析者で構成されたチームです。このリサーチ・チームは、IBM が管理してモニターするエンドポイントのイベント・データ、アクティビティー、トレンドを含め、内部および外部の数多くのソースから、セキュリティー・データを分析しています。

目次

概要: 公表された金融インシデント

IBM X-Force インタラクティブ・セキュリティー・インシデント・データは、公表された重要なインシデントのサンプリングです。[4] これには、データの流出につながったインシデントである漏えいが含まれています。図 2 が示すように、2016 年には、サイバー攻撃に誘発された経済的破綻が尽きることがありませんでした。分散サービス妨害 (DDoS) による障害で、オンライン金融機関の運用が世界中でシャットダウンされました。ランサムウェアなどのマルウェアが、何百万もの損失の原因となっています。SWIFT 攻撃の標的となったある銀行では、顧客の口座から 8,100 万米ドルが盗まれました。[5]

また、攻撃者は、多様なフィッシング手法から以前よく使用されていたビジネス・メール詐欺 (BEC) に戻って、うっかりした被害者から金銭をだまし取っています。これは、被害者にとって大問題ですが、現在の保険で対象となりにくいため、その百万ドル規模の詐欺に使用された銀行にとっても問題となっています。金銭的な損失に加えて、多くの不正アクセスにより、高度の機密金融データの漏えいが発生しています。銀行のある 1 件の不正アクセスでは、1.4GB の漏えいしたデータに、内部の企業ファイルや顧客の金融データが含まれていたと報告されています。[6]

2016 年には、2 億件以上のレコードが不正アクセスされました。合計 2000 万件未満だった 2015 年から、937 % の増加に当たります。これにより、金融サービス・セクターは、漏えいレコード件数で第 3 位の業界となりました。IBM X-Force が追跡した公表インシデント件数では、近年の総数前年比は横ばい状態で、公表インシデントは 2014 年に 22 件、2015 年に 21 件、2016 年に 22 件でした。

目次

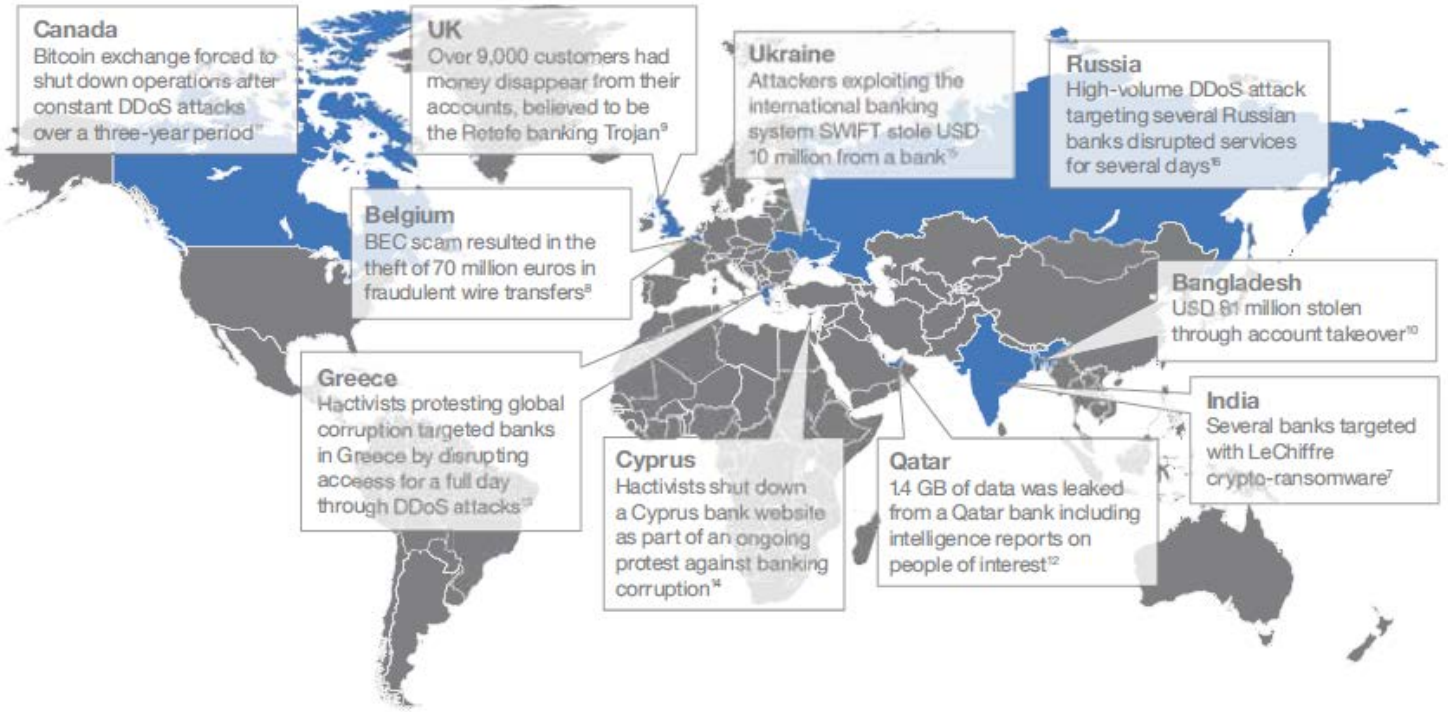

図 2. 2016 年に金融サービスで公表された大きなセキュリティー・インシデント。出典: IBM X-Force インタラクティブ・セキュリティー・インシデントのデータ。

目次

「悪者」はどこにいるか? 内部者か、外部者か

セキュリティー・エグゼクティブが率いるチームは、毎年、数多くの攻撃に対処しています。防御対象と予算に優先順位を付けるために、脅威がどこから来るかを継続的に監視しています。攻撃は、そのほとんどは外部からのものなのでしょうか、あるいは、組織の攻撃全体の大半は内部者が占めているのでしょうか?

攻撃元が組織の内部か外部かを判別するために、セキュリティー調査チームはまず、ソース IP と宛先 IP が内部か、外部かを特定します。その後、関連の攻撃パターンを調べて、悪意のあるものか、不注意によるものかを判定します。IBM Managed Security Services (MSS) の 2016 年の金融サービス・セクターに関するデータ (図 3 を参照) では、組織に影響を及ぼしたのは、内部者の攻撃のほうが外部者より多い (58 % と 42 %) ことが明らかになっています。また、内部者のグループの中で、不注意な操作者 (53 %) のほうが、組織に反して行動した悪意のある内部者 (5 %) より圧倒的に多くみられました。

2017 年の「IBM X-Force Threat Intelligence Index」によると、標的となった上位 5 つの業界である小売、医療、製造、金融サービス、情報通信の中で、2016 に金融サービス業界では、不注意な操作者から最も高いレベルの脅威が発生しています。後で詳しく説明する「アクセス制御の破壊」の攻撃タイプのように、不注意な操作者とは、そのユーザーが意識せずに、感染したシステムが攻撃を実行する状態と考えることができます。悪意のあるメール添付、クリックジャッキングまたはフィッシング、あるいはネットワークで接続された別の内部システムから攻撃された脆弱なコンピューター・サービスによってデスクトップ・クライアントが感染したときに、これが多く発生します。

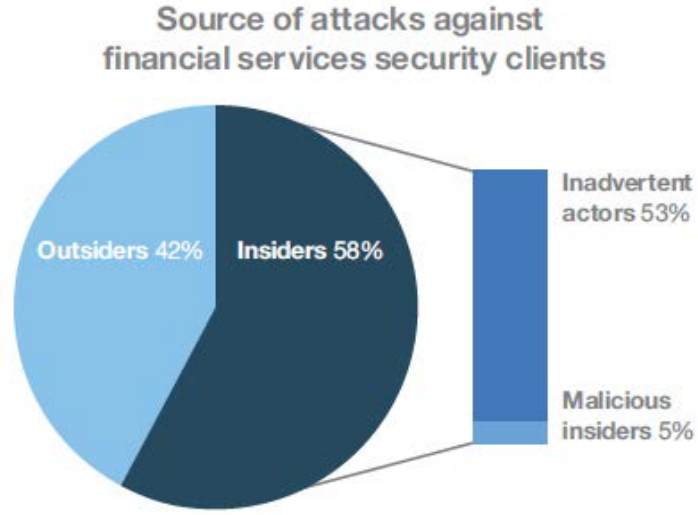

図 3. 2016 年、金融サービス・セクターの攻撃は、外部者より内部者のほうが多く原因となっていました。

金融サービスのモニター対象クライアントで多く使用されていた攻撃方法

金融関係に影響する脅威のタイプを分類して理解しやすくするために、X-Force では、The MITRE Corporation の CAPEC™ (Common Attack Pattern Enumeration and Classification) の基準に従って、2016 年に観測された攻撃タイプをグループ分けしています (図 4 を参照)。MITRE の説明にあるように、「脆弱性を悪用する際によく使用されるメカニズムに基づいて、攻撃パターンを体系化しています」。ただし、「インディケーター」のカテゴリーだけは例外です。これは、脅威および攻撃パターンの条件、状況を記述するものです。

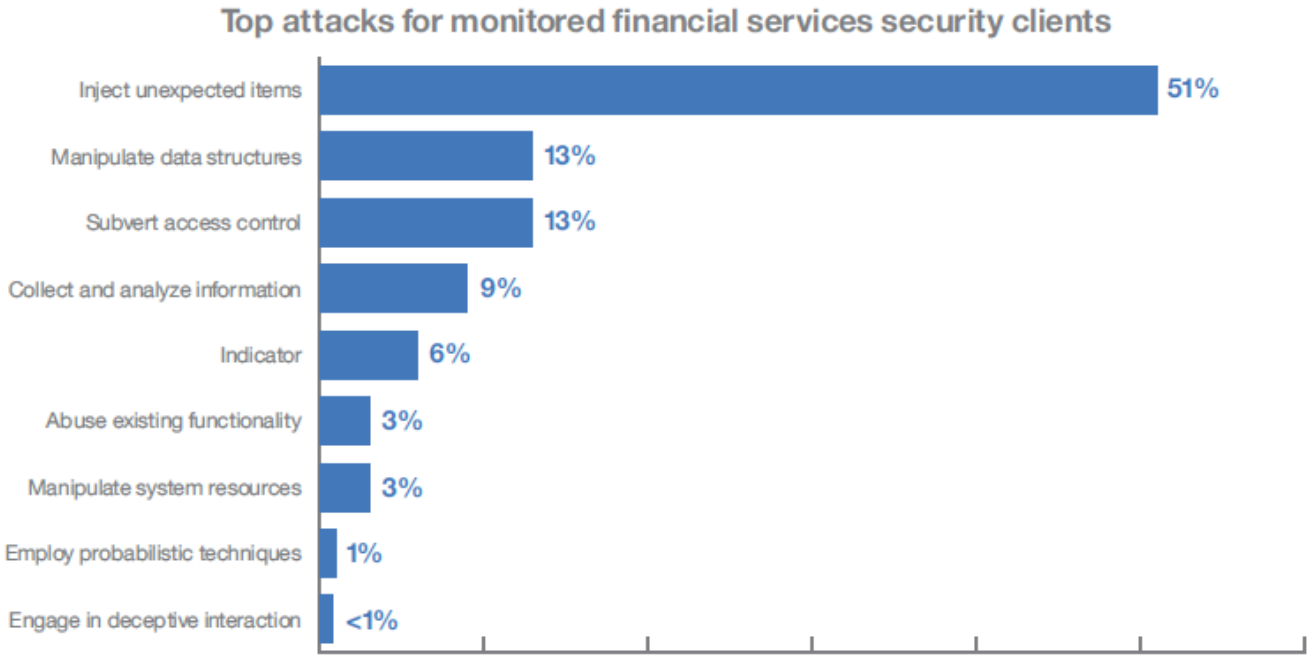

図 4. 2016 年の金融サービス・セクターでは、インジェクション・タイプの攻撃が圧倒的に首位を占めました。出典: IBM Managed Security Services のデータ、2016 年 1 月 1 日 - 12 月 31 日。

目次

以下のセクションに、各攻撃タイプの詳細を示します。

予期しないアイテムのインジェクション

2016 年の IBM MSS データの分析によると、第 1 位の攻撃ベクトルは、システムの制御または破壊を図る悪意のある入力データの使用に関連するもので、IBM X-Force がモニターする金融サービス・クライアントの 51 % が標的になりました。この数字は、全業界平均の 42 % を大きく上回っています。

オペレーティング・システム・コマンド・インジェクション (OS CMDi) や SQLi などのコマンド・インジェクションは、このカテゴリーに属します。OS CMDi は「シェル・コマンド・インジェクション」とも呼ばれます。現在、広まっていて悪名高い Shellshock の脆弱性は、ここから命名されたものです。Shellshock の使用は、出現から 2 年となる 2016 年 9 月を前に全業界で急増し、2016 年の金融サービス組織を標的にした全攻撃の 4 分の 1 を超えています。

SQLi と OS CMDi がこのセクターで最も使用されている攻撃ベクトルであるのは、これらの脆弱性の悪用に成功すれば、機密データの読み取り、変更、破壊が可能になるためと考えられます。金融機関データベースの個人情報 (PII) は、ハッカーにとって高い価値があります。この個人情報を売って高い収入を得ることも、これをもとに、金融機関が取り戻すため、または公表されないようにするための身代金を要求することもできます。

データ構造の操作

第 2 位の攻撃ベクトルは、攻撃者がシステム・データ構造を操作して不正アクセスを図る攻撃に関わるものです。CAPEC™ によると、「(バッファー・オーバーフローの脆弱性などの) 脆弱性や、こうしたデータ構造の悪用可能性は、その設計や規定処理におけるあいまいさや想定に原因があります。」[17] このカテゴリーの攻撃の大半は、バッファー・オーバーフローの脆弱性を標的にしていました。

明るい話題としては、このカテゴリーの攻撃に関する全業界クライアントの平均は 32 % であり、金融サービス・セクターでは 13 % と、かなり低い数字となっています。これは、この攻撃ベクトルが金融サービスの標的に対しては成功率が低いと、攻撃者が見ていることが理由である可能性があります。

アクセス制御の破壊

攻撃の 13 % を占め、全業界平均の 3 % よりかなり高い第 3 位の攻撃ベクトルは、「ID と認証の管理に標的が利用するメカニズムでの弱点、制限、想定を悪用」してアクセス制御を破壊しようとする攻撃に関するものです。[18]

このカテゴリーで観測した攻撃のほとんどは、正当なクライアントであるとサーバーが信じる際の暗黙的信頼を利用して、標的のクライアント/サーバー間通信チャネルにおける認証とデータ整合性の脆弱性を悪用するものでした。

攻撃者が 2 者間 (ユーザーまたはシステム) のメッセージをインターセプトしてリレーしようとする中間者攻撃 (MITM) は、 このカテゴリーに入ります。この手法では、攻撃者が、双方向に流れている情報を盗んだり、接続に悪意のあるコードを挿入したりすることを可能にします。一部のモバイル・バンキング・アプリが、データ送信方法を誤り、MITM の攻撃に弱いことが分かりました。[19]

情報の収集と分析

情報の収集と盗用に焦点を当てた攻撃は、クライアント・デバイスを標的にした攻撃のほぼ 9 % を占めました。これらのほとんどは、既存の弱点を発見するために潜在的な標的の情報を収集する一種の偵察とよく見られる、フィンガープリントに関するものです。基本的に、攻撃者は、標的システムの出力と、標的に関する詳細 (オペレーティング・システムやアプリケーションのタイプやバージョンなど) を固有に識別する既知の「フィンガープリント」を比較します。攻撃者は、この情報を利用して、標的組織の IT インフラストラクチャーで既知の脆弱性を識別し、戦術を練るのです。

インディケーター

「インディケーター」は、CAPEC™ の攻撃メカニズムではありません。サイバー脅威のインディケーターは、いくつかの観測可能な条件と、その条件またはパターンに関する状況情報から構成されます。これらのイベントは、全攻撃の 6 % を占め、標的システムへの攻撃の試行または成功を示している可能性があります。この攻撃の多くは、短時間で 100 回以上の外部 ping が発生した標的システムに関するもので、これは、内部ホストの感染を示している場合があります。ホストが感染していれば、それが検出されて阻止されるまで、他の標的を攻撃したり、他の感染ホストとやり取りしたりする可能性があります。

既存機能の悪用

攻撃の 3% は、「アプリケーションの本来の意図ではない悪意のある目的を達成するため、または標的の機能に影響が出る程度までにリソースを枯渇させるために、アプリケーションの 1 つ以上の機能を」悪用または操作しようとすることに関係しています。[20] このカテゴリーの攻撃が成功すると、攻撃者は、機密情報を入手したり、サービスを妨害したり、標的で任意のコードを実行したりできます。

システム・リソースの操作

システムのリソース状態または可用性について何らかの操作をしようとする攻撃は、全攻撃の 3% を占めました。リソースには、ファイル、アプリケーション、ライブラリー、インフラストラクチャー、構成情報などがあります。このカテゴリーの攻撃が成功すると、攻撃者は、サービスを妨害したり、マシンを感染させてボットネットの C&C (command-and-control) サーバーにしたり、標的で任意のコードを実行したりできます。

確率的手法の使用

攻撃の 1% は、CAPEC™ で「標的のセキュリティー特性を探って潜り抜ける確率的手法」と言われた方法を使用した攻撃者に関するものです。[21] そのほとんどは、侵入者がユーザー名とパスワードの組み合わせを推測してシステムやデータに不正アクセスする方法である、総当たりパスワード攻撃が関係しています。X-Force が観測した攻撃の大部分は、セキュア・シェル (SSH) サービスが標的でした。SSH はセキュア・リモート・アクセスが可能なため、ユーザーによく利用されます。その一方で、ネットワークを介したシェル・アカウント・アクセス権限を攻撃者に与えてしまう可能性もあります。

偽装の対話

1% 未満の攻撃は、クリックジャッキング攻撃など、スプーフィングによってアクションを被害者に実行させようとするものでした。このタイプの攻撃では、攻撃者が被害者のクリック・アクションを乗っ取り、被害者にさらなる攻撃を起動する可能性もあります。

目次

推奨事項と緩和策

従業員意識教育の重視と継続的な実施

BEC 詐欺やその他のフィッシング詐欺について、教育を通して意識を向上させてください。従業員の教育には、ビデオ、Web セミナー、対面教育など、さまざまな方法を利用できます。フィッシング攻撃をシミュレートするプログラムで、定期的に従業員をテストすることもできます。疑いのあるメールは、調査のために報告するよう、従業員に意識付けてください。

コグニティブ・アプローチによるフィッシング・サイトの検出

金融サービス業界では、不注意な操作者、つまり、標的組織の環境に脅威をうっかり導いてしまったユーザーによる攻撃の割合が相対的に高くなっています。スピアフィッシングの犠牲になるのは、不注意な操作者の最大の弱みの 1 つです。従業員がマルウェアをダウンロードして攻撃者への最初のドアを開いてしまったり、企業の資格情報を盗む偽の Web サイトに従業員を導いたりする可能性があります。

IBM X-Force のデータによると、資格情報の 70 % は、フィッシング攻撃の最初の 1 時間に盗まれます。[22] フィッシング攻撃に正しく迅速に対応するためには、機械学習とコグニティブ・コンピューティングを組み込んで、フィッシングの検出と保護の速度と規模を向上させる必要があります。関連のフィッシング攻撃の発生時にそれを検出し、顧客にアラート通知できるコグニティブ・エンジンが、現在、IBM Trusteer Rapport® で利用可能です。

この新しいコグニティブ・エンジンでは、疑いのある Web サイトからの非構造化データ (リンク、イメージ、フォーム、テキスト、スクリプト、DOM データ、URL など) を分析します。コンテンツ分析をすり抜けるためにイメージをユーザーに表示するだけのものや、Web クローラーを回避するためにページに動的コンテンツを配信するものなど、さまざまなフィッシング・ページを正確に識別することが可能です。サイトで使用されたテキスト、言葉遣い、ロゴなどを分析することで、正確にターゲットのブランドを詳細に指摘して、ロゴの使用が正当なものか、疑念があるものかを見分けることができます。

内部者の脅威のリスクを削減

フィッシングを減らすことは、不注意な操作者による脅威の削減の鍵となります。一方、内部者の脅威に晒されないようにするために、金融サービス組織は、データ・セキュリティーと ID およびアクセス管理のソリューションを組み合わせて、機密データを保護し、許可されたすべてのユーザーのアクセスを管理する必要があります。

目次

機密情報にアクセスできるユーザーが増えるほど、悪意の有無にかかわらず、リスクは高まります。企業は、必ず、情報が絶対的に必要なユーザーにのみアクセスを制限し、時間とともにユーザー人口が変わって増加しても、常に最新の管理を行うようにする必要があります。同様に、情報へのアクセスが容易になり、情報が多くの場所に置かれるほど、内部者、または盗んだ資格情報を持つ外部者が、不適切な理由でその情報にアクセス可能になる確率が高まります。

IBM Security Privileged Identity Manager など、ID 管理機能やアカウント・プロビジョニングのコンポーネントを含むソリューションを利用すれば、さまざまなシナリオで特権 ID の使用を集中管理し、監査することができます。IBM Security Guardium® のようなソリューションでは、機密データを適切に保護することができます。

従業員による規則を守らない行動のリスクを管理する事前対応アプローチを採り入れた IBM Surveillance Insight for Financial Services などのソリューションは、重要です。チャット・トランスクリプト、メールのやり取り、音声録音などの非構造化データを取り込み、それを構造化されたトレード・トランザクション・データと組み合わせることができるソリューションでは、堅牢な統合監視システムを構築できます。

サイバー・セキュリティー・インテリジェンス機能の強化

セキュリティー・インテリジェンスは、全業界セクターで必要ですが、金融サービス・セクターでは特に重要です。最も攻撃されやすい攻撃ベクトルを把握することは不可欠です。この情報があれば、金融サービスの企業は、常に犯罪者の一歩先に立ち、内部および外部の検出・保護メカニズムを強化することができます。

しかし、セキュリティー運用チームは、自分の組織を標的とした無数の脅威や増加し続ける攻撃にどのようにしてついていくのでしょうか? 最新の脅威インテリジェンスを常に得ることは、リスク認識の重要な部分です。しかし、脅威データのスピードは、人間の能力をはるかに超えています。高度なスキルを持つセキュリティーのプロフェッショナルでも、莫大なセキュリティー・インシデントや利用可能な脅威データを調べるのは困難です。IBM QRadar® Advisor with Watson® など、コグニティブ機能と分析を組み合わせたソリューションでは、ブログ、Web サイト、調査報告などの大量の非構造化データを活用して、関連するセキュリティー・インシデントに関連付けることで、セキュリティー・アナリストによる複雑な脅威の識別と理解を支援します。

目次

コストと複雑性を軽減しながら企業を保護

インフラストラクチャー、データ、アプリケーションの保護から、クラウド、マネージド・セキュリティー・サービスに至るまで、IBM Security Services には企業の重要資産を保護するための専門知識が盛り込まれています。IBM では、世界でいくつかの複雑なネットワークを保護し、ビジネスで最高レベルの知性を投入しています。

IBM は、セキュリティー・プログラムの最適化、高度な脅威の阻止、データの保護、クラウドおよびモバイルの安全保護を図るサービスを提供しています。Security Intelligence Operations and Consulting Services では、セキュリティーのベスト・プラクティスと対比して、お客様のセキュリティー・ポスチャーと成熟度を評価します。IBM X-Force Incident Response and Intelligence Services では、IBM のエキスパートが、脅威を事前に捕らえて対応し、漏えいが発生する前に最新の脅威インテリジェンスを適用します。IBM Managed Security Services では、セキュリティー・ポスチャーを向上できる業界最高レベルのツール、セキュリティー・インテリジェンス、専門知識を利用できます。多くの場合、自社構築のセキュリティー・リソースよりコストを大幅に抑えることができます。

IBM Security について

IBM Security では、エンタープライズ・セキュリティーの製品およびサービスの高度な統合ポートフォリオを提供しています。世界的に有名な IBM X-Force リサーチによってサポートされるポートフォリオは、組織でユーザー、インフラストラクチャー、データ、アプリケーションを総合的に保護できるようにセキュリティー・インテリジェンスを提供し、ID およびアクセス管理、データベース・セキュリティー、アプリケーション開発、リスク管理、エンドポイント管理、ネットワーク・セキュリティーなどのソリューションを提供します。IBM は、世界最大級の規模を誇るセキュリティー研究・開発・提供機関を運用しており、130 カ国以上の国々で 1 日当たり何十億件ものセキュリティー・イベントを監視し、3,500 件以上のセキュリティー関連の特許を保持しています。

IBM Security

著者について

Michelle Alvarez は、IBM Managed Security Services の脅威リサーチャー/エディターで、10 年を超える業界経験を職務に生かしています。Michelle は、セキュリティーのトレンドのリサーチと分析、セキュリティーおよび脅威緩和に関するソート・リーダーシップ・ペーパーの作成と編集を担当しています。2006 年の Internet Security Services (ISS) の買収により、IBM に入りました。ISS では、アナリストとして、 世界で最も包括的な脅威および脆弱性データベースの 1 つである X-Force データベースの開発に貢献しました。Michelle は長年、情報技術分野のメンバーで構成される非営利有限責任会社の Information Technology-Information Sharing and Analysis Center (IT-ISAC) で運営の重要な役割を担っていました。現在、IBM 提供のセキュリティー・ブログ SecurityIntelligence.com のレギュラー寄稿者で、情報技術で修士号を取得しています。

詳細情報

IBM Security ポートフォリオの詳細については、IBM 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、以下をご参照ください。
ibm.com/security

セキュリティー・サービスについて詳しくは、以下をご参照ください。
ibm.com/security/services

Twitter で @IBMSecurity をフォローするか、IBM セキュリティー・インテリジェンスのブログをご覧ください。

IBM

目次

1 https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SE912353USEN

2 https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SE912353USEN

3 http://money.cnn.com/2016/05/20/news/swift-bank-attack-global-ecuador/

4 http://www-03.ibm.com/security/xforce/xfisi/

5 https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know/

6 http://www.bankinfosecurity.com/qatar-national-bank-suffers-massive-breach-a-9068

7 http://news.softpedia.com/news/lechiffre-ransomware-hits-three-indian-banks-causes-millions-in-damages-499350.shtml

8 http://www.net-security.org/secworld.php?id=19370

9 http://www.independent.co.uk/news/business/news/tesco-bank-accounts-suspended-transactions-access-frozen-hack-money-la-a7402006.html

10 http://thehackernews.com/2016/04/bank-firewall-security.html

11 https://www.hackread.com/bitcoin-exchange-ddos-attacks/

12 http://www.databreachtoday.com/qatar-national-bank-suffers-massive-breach-a-9068

13 https://www.hackread.com/anonymous-ddos-attack-bank-greece-website-down/

14 https://www.hackread.com/oplcarus-hacktivists-ddos-central-bank-of-cyprus/

15 http://thehackernews.com/2016/06/ukrainian-bank-swift-hack.html

16 http://www.theregister.co.uk/2016/11/11/russian_banks_ddos/

17 https://capec.mitre.org/data/definitions/255.html

18 https://capec.mitre.org/data/definitions/225.html

19 http://news.softpedia.com/news/76-ios-apps-including-medical-and-banking-tools-are-exposing-data-to-hackers-512693.shtml

20 https://capec.mitre.org/data/definitions/210.html

21 https://capec.mitre.org/data/definitions/223.html

22 https://securityintelligence.com/hey-phishing-you-old-foe-catch-this-cognitive-drift/

IBM Security

目次

IBM セキュリティー
日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町 19 番 21 号

Produced in the United States of America
2017 年 4 月

SEL03129-JPJA-00