中堅・中小企業のための エンタープライズ・レベルのセキュリティ

概要

今日、EメールとWebは、多くの組織にとって業務に必要不可欠なツールとなっています。その結果、ほとんどのサイバー攻撃は、EメールまたはWeb経由で始まることになります。また、組織をサイバー攻撃から確実に守るためには、既知の一般的な攻撃と同様、未知の高度な攻撃も検知、防御できなければなりません。業界で高い評価を得ているFireEyeのテクノロジーは、複数の経路から段階的に実行される高度な複合型サイバー攻撃の検知と防御に大きな効果を発揮します。誤検知も最小限に抑えられており、効果的・効率的な運用が可能です。FireEyeのソリューションは容易に利用できるよう設計されているため、お客様は運用管理に多大なリソースを割くことなく、自社本来のビジネスに注力できます。

FireEyeが他社に先駆けて開発した高度で未知のサイバー攻撃を検知するテクノロジーは、これまで、大企業に導入されるケースがほとんどでした。しかし、今日のサイバー攻撃者は、規模を問わずあらゆる組織を標的にしています。対岸の火事だとサイバー攻撃を軽視していると、中堅・中小企業（SME）も予想外の被害を受けかねません。自社への攻撃に備えて、高度な脅威対策を既存のセキュリティ・フレームワークに追加する必要があります。

SMEが抱える課題

SMEは、セキュリティに関するさまざまな課題に直面しています。その大部分が、絶え間なく変化するセキュリティ脅威トレンド、または組織におけるセキュリティ・オペレーションのあり方のいずれかに関係しています。

セキュリティ脅威トレンドに起因する課題の多くは、「組織全体のセキュリティ状況を可視化できていない」という点に原因があります。また、シグネチャ・マッチングに依存する従来型の境界セキュリティ・テクノロジーでは、最新のセキュリティ脅威の検知は実現できません。攻撃者は、シグネチャによる検知を回避するために、攻撃のたびにマルウェアの特徴を変化させ、同じマルウェアを複数の組織で使用しないように心がけています。さらに、マルウェア自体をまったく使用しない攻撃すらあります。

セキュリティ運用に関する課題の多くは、「手動での対応を必要とするセキュリティ・アラートが大量発生しているにもかかわらず、そのための人手が不足している」という現実から生み出されています。セキュリティ・ソリューションが発するアラートの多くは誤検知であり、アナリストの貴重な時間は無害なイベントの調査という無駄な作業に費やされてしまいます。この問題には、誤検知の山に埋もれた重大なアラートが見逃され、その結果、深刻なイベントへの対応が遅れ被害が拡大してしまうという弊害もあります。

状況はさらに複雑です。アラートを調査するためには、適切な専門知識を備えた人材を雇用する必要がありますが、SMEのセキュリティ担当者はIT部門に所属しているケースが多く、セキュリティ・オペレーションだけに専念することは困難です。また、多層防御戦略を採用している場合には複数のセキュリティ・ツールを運用する必要がありますが、リソースに余裕のないSMEでは、ツールの管理をサービス・プロバイダーに任せる、社内で管理しているが適切になされていない、まったく管理していない、のいずれかのシナリオに行き着くのが一般的です。その結果、最善のケースでも多大なコストが発生し、最悪のケースでは深刻なセキュリティ・リスクに直面することになります。多くのSMEは、ここに挙げたすべての問題を抱えています。つまり、膨大なアラートを発する多数のセキュリティ・ツールをごく限られた人材で管理しながら、コストの抑制を図らなければならないのです。

FireEye

ソリューション

FireEye Network Security Essentials（NXE）とEメール脅威対策クラウド（ETP）を組み合わせたソリューションでは、サイバー攻撃の90%を占めるWeb経由の攻撃とEメール経由の攻撃の両方に対応できます[1]。このソリューションでは、的確で迅速なインシデント対応を妨げる誤検知が最小限に抑えられます。重大なインシデント発生時を除いてアラート数が大幅に減少するため、SMEの限られたセキュリティ・リソースを最大限に有効活用できます。

これらのFireEyeテクノロジーの中核を構成するのは、強力な検知技術であるFireEye Multi-Vector Virtual Execution™（MVX）エンジンです。MVXエンジンは、WebやEメールなど複数の経路から段階的に実行され、個別の解析では見逃す恐れのある複合型の攻撃を検知します。

複数の経路から実行される複合型の攻撃は、不正なEメールから始まるケースが一般的です。したがって、攻撃の発生を検知するためには、不正なURLとスピア・フィッシング・メールの相関分析が重要となります。Cloud　MVXエンジンは、分析の結果に基づいて2つのイベントの関係性を判断し、その後に展開される攻撃活動（ネットワークで収集したデータをWeb経由で外部に送信するなど）を自動的に阻止します。ここで得た情報は、同様の戦術、ツール、手順（TTP）を使用する別の攻撃の検知および防御にも役立ちます。

自動化と効率化を高レベルで実現するこのソリューションでは、組織のセキュリティ体制を強化しながら、ネットワーク・セキュリティとEメール・セキュリティの導入および日常的な運用管理を簡素化できます。

Network Security Essentials

Network Security Essentialsは、手頃な価格で導入できるプラグアンドプレイ型のネットワーク・セキュリティ・ソリューションです。わずか1時間ほどで導入を完了し、深刻なセキュリティ侵害の発生リスクを最小限に抑えることができます。

Network Security Essentialsは、シグネチャに依存しない特許取得済みの検知技術Cloud MVXエンジンに加え、既知および未知のセキュリティ脅威を検知、ブロックするIntelligence-Driven Analysisテクノロジーを搭載しています。コンテキストに基づくルールベース・エンジンの集合体である同テクノロジーは、マシン、攻撃者、被害者に関する最新情報に基づいて、不正な活動を検知、ブロックします。また、侵入防御システム（IPS）を搭載しており、一般的な攻撃にはシグネチャ・マッチング技術で対処するほか、リスクウェア対策技術でスパイウェアやアドウェアをブロックできます。従来型や次世代型のファイアウォール、単機能のIPSソリューション、アンチウイルス・ソリューションと異なり、誤検知を最小限に抑えながら、既知および未知の攻撃（ゼロデイ攻撃）を正確に検知します。このため、セキュリティ担当者は、確実に重要なアラートへの対応に専念できます。

柔軟に選択できる導入形態

Network Security Essentialsの導入には、オンプレミスの仮想アプライアンスまたは物理アプライアンスが必要となります。どちらの場合も、インライン・モードまたはモニター・モードで導入可能です。オンプレミスのアプライアンスであるNetwork Smart Nodeは、プライマリ・ネットワークの境界から支社・支店環境に至るまで、インターネットに直接アクセス可能な幅広い環境に導入できます。物理アプライアンスと仮想アプライアンスでは、コスト・パフォーマンスに優れ、いつでもイメージとしてダウンロードできる仮想アプライアンスのほうが広く利用されています（図1）。Network Smart Nodeは、Intelligence-Driven Analysisテクノロジーとシグネチャベースの IPSを併用して、疑わしい活動を検知、ブロックします。詳細解析が必要なオブジェクトが見つかった場合には、FireEyeのプライベート・クラウド上のCloud MVXサービスに暗号化接続で送信し、調査を実施します。Network Smart NodeとCloud MVXサービスは、統合ハードウェア・アプライアンスとしても利用可能です（図2）。小規模環境には50Mbpsのモデル、中規模環境には100 Mbpsのモデルを推奨します。

Eメール・セキュリティ：Eメール脅威対策クラウド（ETP）

大規模なセキュリティ侵害事件の多くは、1通のEメールがきっかけとなっています。ETPは、Eメールを解析して、一般的なウイルスやスパムの脅威、さらにスピア・フィッシングの可能性を検証するクラウドベースのSoftware-as-a-Service（SaaS）サービスです。特許技術のCloud MVXテクノロジーを使用するETPは、高度なEメール攻撃を予防的に防御します。インラインのアンチスパムおよびアンチウイルス機能を備えるほか、オンプレミスとクラウドの両メールボックスをインライン・モードまたはモニター・モードで保護できます。

脅威インテリジェンス

FireEyeのソリューションでは、通常のアラートと補完する脅威インテリジェンスがクラウド経由で配信されます。1時間おきに更新される脅威インテリジェンスには、新種のマルウェア、脆弱性を突くエクスプロイト、攻撃者と被害者、新たに確認された脅威に関する情報が含まれています。クラウド解析技術と機械学習テクノロジーでCloud MVXエンジンを補完するこの脅威インテリジェンスにより、高度な脅威も逃さず検知できるようになります。以上のように、FireEyeのソリューションでは、推定される攻撃者の素性やその目的、マルウェアの詳細などの重要なコンテキスト情報が状況に応じて提供されるため、既知のマルウェアに限らず標的型のゼロデイ攻撃も検知、防御できます。

[1] Verizon 2015 Data Breach Investigations Report

ソリューションの構成例

ソリューションの構成時に考慮すべき点としては、監視対象とするEメール・アカウント数、システムを通過するネットワーク・トラフィック量、仮想環境か物理環境か、クラウド・サービスの利用の有無、経営幹部や取締役会のセキュリティ意識のレベルなどが挙げられます。FireEyeとパートナーは、これらの構成例をベースに、お客様のニーズに合ったソリューションの選択や設計をお手伝いします。

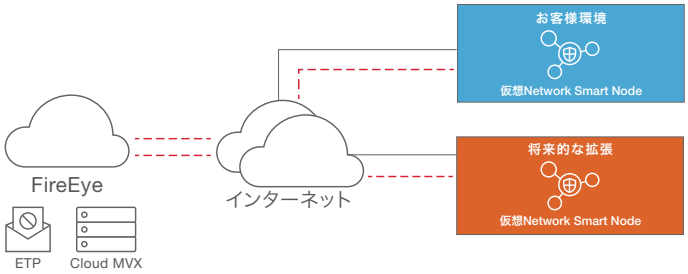

図1：ETPクラウド、Cloud MVX、仮想アプライアンス

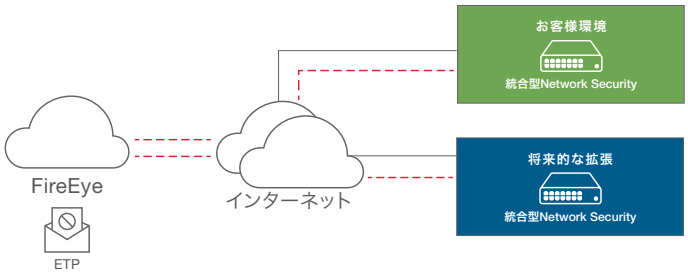

図2：ETPクラウド、物理的な統合型Network Security アプライアンス

	小規模1	小規模2	中規模1	中規模2
導入タイプ	仮想/クラウド	物理アプライアンス	仮想/クラウド	物理アプライアンス
社員数	200～250	200～250	450～550	450～550
ネットワーク・トラフィック	50 Mbps	50 Mbps	100 Mbps	100 Mbps
ソリューションの例	ETP 200～250ユーザー 仮想NX1500 Cloud MVX	ETP 200～250ユーザー 統合型2500NXE1	ETP 450～550ユーザー 仮想NX2500 Cloud MVX	ETP 450～550ユーザー 統合型2500NXE2

次のステップ

リソースが限られセキュリティ意識が不足気味のSMEはセキュリティ対策が不十分になりがちで、高度なサイバー攻撃者の格好の標的となっています。SMEがリスクを抑えながらビジネスの拡大を図るためには、基本を踏まえた一定レベルのセキュリティが欠かせません。その実現には、セキュリティの状態やセキュリティ・プログラム、ツール、プロセスに確固たる自信が持てる、エンタープライズ・レベルの体制構築が重要となります。

FireEye製品の詳細については、次のWebページをご覧ください。
www.FireEye.jp

ファイア・アイについて

FireEye®は、インテリジェンス主導型のセキュリティ企業です。顧客企業は、FireEyeの革新的セキュリティ技術、国家レベルの脅威インテリジェンス、世界的に著名なMandiant®コンサルティングの知見が統合された単一プラットフォームを、自社のセキュリティ対策の一部としてシームレスに組み込むことができます。FireEyeは「Forbes Global 2000」企業の4割以上を含む、世界67か国以上の6,000を超える組織で利用されています。

ファイア・アイ株式会社 | 〒101-0054 東京都千代田区神田錦町3-22 テラススクエア8階 |
03−4577−4401 | Japan@fireeye.com | www.fireeye.jp
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 |
877.FIREEYE (347.3393) | info@fireeye.com | www.FireEye.com