お客様事例

FireEye

米ノースショア公共事業区：厳格化された連邦政府要件にFireEyeで対応

概要

業種

官公庁

お客様の概要

米国ワシントン州シアトルのすぐ北に拠点を構えるノースショア公共事業区（NUD）は、地区の上下水道を運営管理する事業体です。6都市44平方キロの地域に居住する住民6万5,000人に水道サービスを提供しています。主要貯水池を5か所、下水道施設を10か所、シアトルの配水網につながる複数の連絡施設を運営するほか、隣接都市と多様な連携の下に、地域の主要病院にサービスを提供しています。

1998年の米大統領指令により、テロ攻撃への対策強化が必要な重要インフラを特定するための国家プロジェクトが立ち上げられました。対象となるのは、救急サービス、通信、エネルギー、金融、水道、食料、運輸など、社会運営の維持に関する事業を支えるあらゆる構成要素です。

時代背景を考えれば当然のことですが、この大統領指令で保護の対象とされていたのは、物理的な要素に限定されていました。しかしその後、サイバー空間での脅威の急増を受け、デジタル資産やインターネットに接続されたインフラも保護の対象に追加されています。

「FireEyeのプラットフォームは、段階的にインストールされるマルウェアが使用された60の事例すべてにおいて、攻撃を正確に検知し、防御してくれました。検知率は実に100%です」

— **スティーブン・ショマー氏**、ITディレクター、ノースショア公共事業区

「当時の私たちのセキュリティ・モデルでは、新しい脅威への対応が困難になっていました」。NUDでITディレクターを務めるスティーブン・ショマー（Stephen Schommer）氏は、以前の状況をこのように振り返ります。NUDでは当時、従来型のファイアウォールとエンドポイント向けのアンチウイルス・ソリューションを導入していました。しかし、APT攻撃（Advanced Persistent Threat：高度で持続的な標的型攻撃）やカスタム・マルウェア、フィッシング攻撃などの高度なサイバー攻撃が増加する中、これらのソリューションには、十分な効果が期待できなくなっていたのです。

また同氏は、SCADA（Supervisory Control And Data Acquisition）システムを含む内部ネットワークや、貯水池などの遠隔拠点、トラック車両、携帯端末（タブレットやスマートフォン）の保護を強化する必要も感じていました。

新たな被害事例とならないために

ショマー氏はまず、一般的な多層防御アーキテクチャを構成するため、当時運用していたファイアウォール・ベンダーが提供するハードウェアベースのVPNソリューションと侵入防御システム（IPS）を導入しました。また、エンドポイントでシグネチャベースのマルウェア・スキャンを実施するよう設定を行い、スパム対策アプライアンスを導入。さらに、ネットワークとインターネットを切り分けるため、DMZ、イントラネット、遠隔地の上下水道施設を管理するSCADA用のネットワークを構築しました。

しかし、ショマー氏は、これだけではまだ不十分だと考えていたのです。たとえば、エンドポイント用のアンチウイルス・ソリューションは、不正な通信や不正なコードの実行を事後的にしか検知できません。また、レポート、ログ、監視の機能も理想からほど遠く、高度化の一途をたどる脅威に対抗できるだけの機能を備えていませんでした。

「これで十分な対策ができたとは思っていませんでした。サイバー攻撃の新たな犠牲者にならないようにと願いながら、何とか持ちこたえているだけでした」とショマー氏は当時の状況を説明します。同氏は、このときすでに、近隣の小都市で起きたマルウェア感染被害の情報を耳にしていました。その都市では、行政、公共事業、警察の施設で運用していたすべてのPCが、マルウェア感染によってボットネットに乗っ取られていたのです。IT部門は、被害を完全復旧するまでに3か月以上の時間を費やしたといいます。また、サイバー攻撃で40万ドルの損失を出した別の都市の事例や、詐欺行為で100万ドル以上を窃取された近隣病院の事例も、同氏の耳に入っていました。

「新たな被害者として、新聞の見出しを飾るような事態は避けたいと思っていました」とショマー氏は振り返ります。「そのためには、最新のアプローチを取り入れた、予防的な多層防御戦略が必要だと考えました」

業界レポートでFireEyeの導入を決断

ショマー氏は、NUDの車両と貯蔵施設に導入している通信トンネルを強化するところから着手したいと考えていました。また、エンドポイントに至るあらゆるコンポーネントに、詳細なレポート機能を導入する必要を感じていました。

そこで自らリサーチを行い、業界レポートを読み込んだ結果たどり着いたのが、FireEyeのソリューションと、Mandiantコンサルティングが提供する業界屈指のインシデント対応サービスです。

特にショマー氏の目を引いたのは、FireEyeネットワーク・セキュリティ（NXシリーズ）プラットフォームが備える振る舞い解析機能とリアルタイムの保護機能です。この両機能は、カスタム・マルウェアやAPT攻撃、ゼロデイ・エクスプロイトなどの高度な攻撃への対応を可能にします。

自身の選択に間違いがないかどうかを確認するため、ショマー氏は、Delta Testingが提供する比較分析レポートに目を通します。FireEyeの優位性は一目瞭然でした。FireEyeは、ゼロデイ脅威の検知率で99.14%を達成していたのに対し、それに次ぐソリューションの検知率は、わずか33.62%だったのです。

スムーズな導入

ショマー氏は、FireEye NXシリーズを各サブネットの出入口にインライン構成で導入しました。「プラットフォームの導入は、非常に簡単でした」とショマー氏は語ります。NXシリーズはデュアル・ポート機能を備えており、DMZの境界とイントラネットを個別に監視できるため、Webエクスプロイト、マルチプロトコルのコールバック、段階的にインストールされるマルウェアをリアルタイムでブロックすることが可能です。

「特に気に入っているのは、未知の脅威を解析する際のアプローチです。FireEye Multi-Vector Virtual Execution（MVX）エンジンは、脅威の動作を隔離環境で解析してその結果をレポートし、クラウド経由で他のFireEye導入環境と共有するのです」（ショマー氏）

NUDでは、ネットワークの両端にVPN用のハードウェア・ファイアウォールを導入していますが、ショマー氏は、そのファイアウォールとイントラネット・スイッチの間にも、最後の防衛ラインとしてFireEyeネットワーク・セキュリティを導入しました。さらに、この投資を最大限に有効活用するため、ローカルおよびリモートのすべてのトラフィックを、本部に導入したFireEyeプラットフォーム経由でルーティングしています。「このようなアーキテクチャを採用したのは、ネットワークから弱点を排除し、FireEyeのソリューションによる業界最高レベルの厳格な検査ですべてのトラフィックをチェックするためです」とショマー氏はその意図を説明します。

インテリジェンスを共有するコミュニティ

NXシリーズは、リアルタイムの脅威と攻撃に関する情報をFireEyeに送信し、グローバルなデータベースにアップロードします。そしてこのデータベースから、最新のセキュリティ問題についての情報がすべてのFireEye導入環境に配信されます。この仕組みにより、NUDも、世界中のFireEye導入環境からほぼリアルタイムで脅威インテリジェンスの提供を受けられます。「最新のインテリジェンスが即座に共有されるため、エクスプロイトに攻撃の時間的余裕を与えずに済みます」とショマー氏は述べています。

NUDでは、NXプラットフォームをインライン構成で導入しているため、ファイアウォールを通過したすべての不正な通信は即座に検知され、予防的にブロックされた後、ショマー氏のチームに報告されます。「導入直後はわずかな誤検知が発生しましたが、いくつかのパラメータを微調整したところ、それも最小限に抑えられるようになりました」。またNUDでは、追加の保護レイヤとして、サブスクリプション・サービスのFireEye as a Service（FaaS）も利用しています。「FaaSで提供される幅広いサービスのおかげで、人材不足のために人件費が高騰するセキュリティ担当者を増員せずに済んでいます。その時点で必要な専門知識とテクノロジーにすぐさまアクセスできるため、コストを抑えながら高度なセキュリティを実現できます」（ショマー氏）

ショマー氏は、ブロックされたサーバーのレポートに基づいて、感染ホストを運用する他の都市や地区、組織の担当者に感染被害が発生している情報を伝えています。また、情報漏えいの可能性を最小限に抑えるため、2ファクタ認証とリモートからのハードウェアレベルの暗号化を導入しました。

Eメールの保護にはFireEye Eメール・セキュリティ（EX）を使用しています。「EXの導入を決断した主な理由は、FireEyeネットワーク・セキュリティの導入効果に満足していたからです」

NUDでは、FireEyeネットワーク・セキュリティ導入後の1年間で、シグネチャベースのアラート12件とIPSイベント220件を、インシデントに発展する前の段階で解決しています。ショマー氏がFireEyeネットワーク・セキュリティについて特に高く評価するのは、発生した攻撃の試みや偵察活動のタイプを正確に見分けられる点です。「NXの情報に基づいて、セキュリティの強化が必要な場所を判断できます。やはり、効果的な対策にはデータが不可欠だということを実感させられます」。また、FireEyeを導入した結果、以前は気づいていなかったセキュリティ問題を発見し、いざ本物のアラートが発生した場合に備えた対策を講じられるようになったといいます。

「FireEye製品が、ランサムウェア攻撃や認証情報の窃取など、Eメールやウェブサイトを経由する重大な標的型攻撃を複数ブロックしてくれたのはつい先日のことです。この結果だけでも、FireEye製品を導入した価値が十分にあったと考えています」（ショマー氏）

「検知されたマルウェアへの対応プロセスを確立しておくことは重要です。脅威を放置して被害を出すような真似は誰もしたくないはずです。FireEyeの導入後は、何が起きても準備はできているという確信を持つことができています」

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

FireEye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。このアプローチにより、FireEyeは準備、防御、インシデント・レスポンスといった、組織がサイバー攻撃対策をするうえでの課題となっていた複雑性や負担を解消します。FireEyeは「Forbes Global 2000」企業の4割以上を含む、世界67か国以上の6,800を超える組織で利用されています。

FireEye