ユーザ事例

シスコのセキュリティ ソリューションでリソースを保護
アリゾナ大学

概要

顧客

アリゾナ大学

業種

教育

ビジネス上の課題

- 大規模なキャンパス ネットワークで自由な情報フローを維持しながら、内部および外部からの攻撃を防止する。

ネットワーク ソリューション

- シスコのスイッチおよびルータの統合型 Intrusion Detection System（IDS; 侵入検知システム）およびファイアウォール ソリューション
- シスコの Virtual Private Network（VPN; 仮想私設網）

ビジネス上の効果

- セキュリティ アラームの件数が大幅に減少し、不正なアクティビティを簡単に検知できるようになった。
- 不要なトラフィックを排除することにより、サービスプロバイダーのコストが低減した。

アリゾナ大学では、シスコのスイッチおよびルータに組み込まれた侵入検知およびファイアウォール ソリューションを利用して、不要なネットワーク トラフィックを排除するとともに、ネットワーク セキュリティ上の脅威にすばやく対処しています。

「IDSM-2 を搭載したときから、1 日あたり 100,000 件以上のアラームが減少しました。そのおかげで、キャリアから購入する必要のある帯域幅の量が減ったのです。」

— アリゾナ大学ネットワーク システム アナリスト、Geoff Poer 氏

ビジネス上の課題

アリゾナ大学は 1891 年、2 人の賭博者と酒場経営者が寄付した 40 エーカーの土地に設立されました。当時は 2 つの学部に 32 名の学生が在籍していました。今日では米国でもトップクラスの教育研究機関の 1 つとなっており、15 の学部で 34,000 名以上の学生が在籍しており、300 の学位プログラムが設けられています。ツーソンにある 357 エーカーという広大なメインキャンパスのほかに、シエラビスタ、フォートホアチュカ、フェニックスに分校があります。

同大学では共同研究体制による学習を奨励しており、3 箇所のキャンパスをまたがって 40,000 以上のノードで構成されるキャンパス ネットワークは、学生と研究者のコミュニケーションを支援しています。このような大規模ネットワークでセキュリティを管理し、アカデミックな環境に付随する大量のインターネット トラフィックに対処するためには、多くの課題が存在します。

アリゾナ大学の場合、エンド システムのセキュリティの責任を各ユーザおよび学部に課しているという実態と、研究分野、所属先、経済母体、およびコミュニティの境界を越えた自由な情報交換を奨励する文化が育っていることで、この問題はさらに複雑化しています。このような環境では、必然的にセキュリティ事故が起こりがちです。しかし、ネットワークは 1 年に 20% ずつ成長し、インターネット トラフィックはその 2 倍の速度で増加しています。これらの現状を踏まえて、同大学では自由な情報フローへの欲求と、セキュリティに関するニーズの両方に対処する必要に迫られました。

このようなネットワーク セキュリティに関する課題に対処するため、同大学では 2000 年にネットワーク管理部門の補佐役としてセキュリティ事故対策チームを発足させました。このチームの目的は、キャンパス ネットワークを電子的な侵犯から守ることと、ネットワークで必然的に発生するセキュリティ事故に対処することです。

アリゾナ大学のセキュリティ事故対策チームは、大企業にあるようなチームと同じように、ウィルス、ワーム、その他の未許可アクセスといったさまざまな脅威に対処することになりました。しかし、企業環境で運営されるチームとは違って、キャンパス チームには、各ユーザのデスクトップ上でセキュリティ ソフトウェア（ウィルス検出、オペレーティング システム パッチ、およびセキュリティ アップデート）を管理する権限がありません。

「エンドポイントを制御できないことが、私たちにとって常にボトルネックなのです。」アリゾナ大学ネットワーク サービス部の副部長、Ted Frohling 氏はこのように語ります。「サービス プロバイダーから着信して壁面ジャックから出て行くまでの範囲なら、ネットワークを管理できます。私たちがコントールできるのは、そこまでです。」

ネットワークへの潜在的な脅威について理解を深め、セキュリティを改善する方法を学ぶ目的で、同大学はシスコシステムズに連絡し、Cisco Secure Consulting Services（CSCS）に Security Posture Assessment（SPA）の実施を依頼しました。SPA は専門のセキュリティ コンサルタントのチームによって実施され、ネットワーク内外のセキュリティの脆弱性を明らかにするとともに、組織が攻撃を検出して対処する能力を分析し、防御対策を提案します。同大学での SPA によってネットワークの脆弱性が多数発見され、ネットワーク セキュリティに資金を投入する必要性が改めて浮き彫りになりました。

ネットワーク ソリューション

2003 年、アリゾナ大学はいくつかのセキュリティ ソリューションについて調査しました。その中には Cisco Catalyst® 6500 シリーズ Intrusion Detection System Services Module（IDSM-2）と Firewall Services Module（FWSM）が含まれていました。これらの製品は、侵入検知機能とファイアウォール機能をスイッチやルータに統合し、Quality of Service（QoS; サービス品質）などのネットワーク機能とセキュリティ機能のシームレスなコラボレーションを実現します。これらの新しいモジュールによって、同大学の急増するトラフィック負荷に対応するとともに、自由なインターネット アクセスを維持しながら不要なトラフィックをブロックすることができます。これらの製品とシスコのサポート サービスを認識したアリゾナ大学では、セキュリティ ソリューションのアップグレードにシスコを選択しました。

Cisco IDSM-2 は、完全な侵入検知機能を Cisco Catalyst 6500 シリーズ経由でネットワーク インフラストラクチャに直結させ、ワームや DoS 攻撃などのネットワーク侵犯からスイッチド環境を保護します。攻撃の着信をブロックしてアラートを生成するアクティブ レスポンス機能は、同大学のニーズに特に適したものです。このアクティブ レスポンスによって、ネットワークは未許可アクセスやネットワークの性能を低下させようとする試みを検知し、一連のルールに基づいて対応します。また、収集したデータに基づく情報を利用して、それ以降の攻撃を防ぎます。

さらに Cisco IDSM-2 は、攻撃、攻撃者、および被害者の詳細な関連付けも行い、攻撃者トップ 10、キャンパス ネットワークにおける被害者トップ 10 といったデータを含むデイリー レポートが管理者に提供されます。一般に競合他社の IDS では、攻撃元の IP アドレスとその標的しか識別されません。

Cisco FWSM は、業界最速モデルの 1 つであり、アリゾナ大学の高レベルのインターネット トラフィックに対応できます。外部からの未許可のネットワーク アクセスを防止するだけでなく、キャンパス ネットワーク内の特定のサブネット、ワークグループ、または LAN に対する未認証ユーザのアクセスも防止します。

機種の選択では、価格も決め手の 1 つになりました。「いくつかの競合製品の価格を調べたところ、シスコのファイアウォール サービス モジュールの価格は同等の製品の半分程度でした。」アリゾナ大学ネットワーク システム アナリスト兼シニアである Bill Phillips 氏は、このように語っています。

Cisco IDSM-2 および FWSM は、大学ネットワークの 2 台の Cisco Catalyst 6506 スイッチに搭載されています。インターネットおよびインターネット 2 のトラフィックはキャンパス エッジにある 4 台の Cisco 7606 ルータを通じてネットワークに着信し、2 台の Cisco Catalyst 6509 スイッチにルーティングされます。Cisco Catalyst 6509 スイッチは、FWSM および IDSM-2 を搭載した 2 台の Cisco Catalyst 6506 スイッチにトラフィックを転送します。これらのセキュア スイッチを通過したトラフィックは、2 台の Cisco Catalyst 6509 コア スイッチに送信され、その他の Cisco Catalyst 6509 スイッチのディストリビューション レイヤに送信されます。

同大学ではさらに、安全な接続性のためにシスコのアーキテクチャを採用し、ネットワーク境界にはフェールオーバー機能を備えた Cisco VPN 3000 シリーズ コンセントレータを、リモート デスクトップにはシスコの VPN ソフトウェア クライアントを配備しました。

ビジネス上の効果

シスコの新しいセキュリティ ソリューションによって、同大学ではネットワーク攻撃に対して迅速かつ効果的に対処できるようになっています。たとえば、Mydoom ウィルスがインターネットに広がったとき、事故対策チームは感染した約 100 台のコンピュータをただちに発見し、ウィルスを除去してネットワークを守る方法をユーザに指示しました。

また、Cisco IDSM-2 により、キャンパス ネットワーク上で外部ユーザに侵害されている大量のクライアント コンピュータのほか、他の 3 つの大学ネットワーク上の侵害されているコンピュータも発見することができました。これらの侵害されたコンピュータを通じて、未認証ユーザがキャンパス ネットワークに不要トラフィックを発生させる可能性があるばかりか、正当なサービス プロバイダー アカウントなしでインターネットにアクセスする可能性があります。「IDSM-2 がなければ、こういった攻撃や侵害されたコンピュータを発見することはなかったでしょう」と Phillips 氏は語っています。

新しいファイアウォール ソリューションは、ネットワークに着信するトラフィック量を減らしてデータ解析を簡素化することによって、Cisco IDSM-2 の利点をさらに高めています。また、ファイアウォール サービス モジュールによって不要トラフィックが大幅に減少した結果、帯域の所要量が削減され、DoS 攻撃が緩和されました。

「IDSM-2 を搭載したときから、1 日あたり 100,000 件以上のアラームが減少しました。」アリゾナ大学ネットワーク システム アナリスト Geoff Poer 氏は、このように語っています。「そのおかげで、キャリアから購入する必要のある帯域幅の量が減ったのです。」

次のステップ

アリゾナ大学では 2004 年後半、数台の Cisco Catalyst 6509 ディストリビューション レイヤ スイッチに Cisco FWSM を追加し、キャンパス ネットワークのセキュリティを強化する予定です。さらに、既存のディストリビューション ルータでの輻輳とセキュリティ上の問題に対処するために、学生寄宿舎をネットワークの残りの部分から切り離す計画もあります。寄宿舎には、Cisco FWSM を搭載した冗長構成の Cisco Catalyst 6509 スイッチを設置する予定です。

また、同大学では侵入検知およびファイアウォール機能を備えた Cisco 7200 シリーズ ルータの導入も検討しています。さらに別の改善項目として、ハンドヘルド デバイス用のワイヤレス インターネットのサポートも検討されており、これが実現すると、メール サーバなど、機密事項を扱う Web サイトをアクセスする Web ブラウザとしてハンドヘルドを使用できるようになります。

同大学では当分の間、ネットワーク境界で不要トラフィックをシャットアウトすることに重点を置きながら、インストール済みのシスコのネットワーキングおよびセキュリティ製品をフルに活用する予定です。シスコのサポート チームとの良好な関係に基づいて、同大学ではシスコの新しいセキュリティ機能および製品のベータ テストも継続する予定です。「シスコのサポートには大きな信頼感があります。何か新しいことを試したいときや、すぐに支援が必要になったとき、サポート チームがただちに対処してくれます」と Poer 氏は語っています。

この強力なサポート関係と効果的なシスコのセキュリティ ソリューションに支えられて、アリゾナ大学は将来にわたってセキュリティ問題に取り組む体制を整えています。

CISCO SYSTEMS

シスコシステムズ株式会社

URL: http://www.cisco.com/jp/
問合せ URL: http://www.cisco.com/jp/go/contactcenter/
〒 107-0052 東京都港区赤坂 2-14-27 国際新赤坂ビル東館
TEL: 03-6670-2992
電話でのお問合せは、 以下の時間帯で受付けております。
平日 10:00 ～ 12:00 および 13:00 ～ 17:00

お問合せ先

05.03