Texas A&M 大学の敵を迎え撃つ戦略

境界線を引かないネットワーク・セキュリティー

Texas A&M 大学は全米最大規模の敷地に 10 の大学施設と数十もの関連施設を抱え、200 を超える建物をつなぐ分散ネットワークを構築しています。このような分散ネットワークを保護するには、境界セキュリティー・ソリューションではまったく対応できません。

全米最大のキャンパスに広がるネットワークを保護するのは、非常に大変な仕事です。問題が発生しても、その問題を検出すること自体が容易ではありません。どこで何が起こっているのか、ネットワークへの影響はどの程度なのか、その脅威をどう解決すべきかを把握するのは、さらに困難です。学生が主要なユーザー基盤である Texas A&M 大学の巨大な分散ネットワークの前では、境界セキュリティー・ソリューションは時代遅れの産物になってしまうのです。

セキュリティー上の課題

ネットワーキング担当アソシエーツ・ディレクターである Willis Marti 氏は、6 万を超えるユーザーの日常使用を促進しながら、大学のインフラストラクチャー全体を保護するという任務を任されました。次のような複数の要因から Marti 氏の課題が形成されました。

- 学期単位でネットワークへの加入やネットワークからの退会が発生するが、それに伴う学生数の変動
- 大学ネットワークの利用ポリシーを施行して、学生と大学を保護する必要性
- 新しい政府規制への準拠
- 絶えず進化するネットワーク・セキュリティーの脅威に対する予防
- ヘルプ・デスクからの要請、トラブルシューティング、保守、アップグレードのほか、絶えず進化するキャンパス・ネットワークの管理に必要なその他の問題など、膨大な業務

Texas A&M 大学は 1876 年に米国初の公的な高等教育機関として設立され、幅広い学術分野と専門分野において知識の発見・開拓・伝達・利用に取り組んでいます。この大学のカリキュラムには、農学および工学のほか、建築学、経営学、教育学、地学、一般教養、医学、自然科学、獣医学などがあります。

Marti 氏は 1990 年以降、同大学のコンピューター・サイエンス学部で、学生への教育や学部のコンピューター運用に積極的に関わっています。Marti 氏は 2001 年に現在のポジションを引き受け、セキュリティーからネットワークまで、そしてリモート・アクセスからインターネットおよびインターネット 2 の接続性の維持まで、キャンパス・ネットワーク全体を監視しています。

Texas A&M 大学の敵を　迎え撃つ戦略

境界線を引かないネットワーク・セキュリティー

Marti 氏とそのチームがセキュリティーに関して非常に真剣に取り組んでいるため、Texas A&M 大学は National Security Association (NSA) Center of Academic Excellence in Information Security Education に指定されました。Marti 氏は、大学院教育課程でネットワーキングを教えながら、ネットワーク・セキュリティー・コースの一部として大学院生を対象に実践ラボも行っています。Marti 氏は、講義の最中でも、ネットワーキング・チームと作業している時でも、「セキュリティーとネットワークを切り離して考えてはいけない」という基本姿勢を貫いています。

全米最大規模の大学ネットワーク

Marti 氏は、ゼロ・ディフェクト (欠陥ゼロ) は不可能であると考えています。これは、多くの業界に当てはまる概念です。例えば、クレジット・カード会社はクレジット・カード詐欺を撲滅できるとは思っていませんし、小売業者も棚卸し減耗を完全に排除できるとは思っていません。目指しているのは、業務に影響を及ぼさない程度にまで脅威のレベルを下げることです。

> *「ネットワーク管理は情報の流れが保たれているかどうかを確認することで、セキュリティーは、ネットワーク・パフォーマンスの影響にかかわらず、リスクの排除にかかわることだ、というのが世間一般の認識です。しかし、それは、間違ったとらえ方です」と、Marti 氏は言います。「セキュリティーとは、問題を軽減する手段なのです。実際に目指すべきは、業務に影響が出ない程度にリスクを引き下げることのできるネットワーク・セキュリティーなのです」*

Marti 氏とそのチームは、可能な範囲で最強のセキュリティーを実現し、新しい脅威やセキュリティー問題の発生時に対応することで、これを実現しています。Marti 氏は、そのポジションにある人ならば当たり前のことかもしれませんが、より適したソリューションを見逃さないように常に注意を配っています。

> *「6 万を超えるユーザーのうち 4 万 5 千人以上が学生で、毎年 25% の入れ替わりがあります。そのため、経営者と従業員という従来のユーザー関係とはまったく異なる課題が生まれます。学生ユーザーは、年がら年中、私が自分で自分のネットワークの中に連れてこなければならないお客様だからです」*

木から森を見る

Texas A&M 大学は、Q1 Labs のフラグシップ製品である QRadar SIEM を採用することに決めました。この製品はセキュリティー情報とイベント管理に関する次世代ソリューションで、これを使うことにより、企業の IT プロフェッショナルは、これまで、さまざまな部門別サイロから別々に提供されていたネットワーク・セキュリティー管理機能を単一フレームワークにまとめることができます。

> *「以前は、完全対応型の従来のセキュリティー・アプローチを採用していました。ファイアウォールをセットアップし、不正な操作を検出する侵入検出システムに頼り、問題が発生したところでそれを解決するという手順を取っていました」と、Marti 氏は続けます。「Q1 Labs は、ネットワークの状態を把握し、問題を事前に (多くは問題になる前に) 特定するという新しいテクノロジーを見せてくれました。Q1 Labs により当社は、問題が発生するのを待つのではなく、事前にセキュリティー対策を講じ、問題を特定して切り離すことができるようになりました」*

QRadar®

境界防御やそれに似たセキュリティー・アプローチは、私の選択肢にはありません。私は自分のネットワークに脅威の半分を引き込まなければならないからです。

– Willis Marti

(Texas A&M 大学、ネットワーキング担当アソシエーツ・ディレクター)

Texas A&M 大学の敵を　迎え撃つ戦略

境界線を引かないネットワーク・セキュリティー

このユニークで費用効果の高いアプローチは、ネットワークやセキュリティー、アプリケーション、ID などに対する意識の高い、他に類のない監視・監査機能を提供します。QRadar は、システム、アプリケーション、およびユーザーの行動をプロファイリングし、正常パターンを学習して、セキュリティー違反、内部ネットワークの誤用、非効率な運用などのさまざまな異常を認識します。QRadar は、異常の発生元を「ネットワーク上の問題」または「セキュリティー上の脅威」として切り離すことにより、実害が発生する前に疑わしいアクティビティーに対応する機会を Texas A&M 大学に提供します。

> *「QRadar では、ネットワーク全体の状態がまず表示されるので、それを確認し、そこから自分で掘り下げていきます。非常にユニークなソリューションです。DDoS 攻撃や新しいワームなどを処理する場合、これが重要です。というのも、QRadar によって表示される状態を確認することで、ネットワークに及ぶ全体的な影響を確認することができ、そこから絞り込みを行って、対処すべき個々のアクターを特定、監視できるからです。これとは対照的に、ほとんどのレポート作成システムは個別の問題に関するレポートを作成しますが、そこから先の相関関係を把握、確立して、全体的な影響を理解する作業は、ユーザーが行わなくてはなりません」*

Marti 氏は、インストール・グループ、エンジニアリング・グループ、システム・グループを 3 大グループとして、適切に統合された 1 つのチームを作り上げています。この 3 つのグループはいずれも QRadar を使用していますが、ネットワーク・セキュリティーを監視するシステム・グループが主なユーザー・グループになっています。QRadar は異常な動きをリアルタイムで検知し、フラグを立てます。エンジニアリング・グループはこれを即時確認し、コンピューター・レベルまたはサーバー・レベルにまで掘り下げて問題の原因を見つけます。QRadar 警告で、ネットワーク管理やネットワーク利用に関する問題の正確な原因が特定されるときに、エンジニアリング・チームも QRadar の有用性を実感しています。インストール・グループは、トラブルシューティングでネットワーク・トラフィックのシャットダウンやインターネット障害の原因を突き止めるのに QRadar を利用します。さらに、インストール・グループはヘルプ・デスクも運営していますが、下級生スタッフはここで問題の特定と解決に QRadar を利用しています。これにより Marti の上級生アナリストたちは、さらに骨の折れる戦略的な作業に時間を割くことができるわけです。

> *「結局、QRadar の素晴らしい点は、ワームやその他の脅威を初期の段階で感知できるという点です。そのため、聞いたこともない新しいワームや攻撃であっても、実際のセキュリティー上の問題に発展してネットワークに広がる前に、食い止めることができるのです。QRadar があれば、脅威の名前や詳細を知る必要はなく、ただそれを止めればよいのです」と、Marti 氏は締めくくりました。*

> *ネットワークを木々の集まりではなく森として見せてくれるというのが QRadar の隠れた価値だと思います*
>
> **– Willis Marti**
> *(Texas A&M 大学、ネットワーキング担当アソシエーツ・ディレクター)*

Q1 Labs
890 Winter Street, Suite 230
Waltham, MA 02451 USA
1.781.250.5800; info@Q1Labs.com
www.Q1Labs.com

Q1 Labs was acquired by IBM in October 2011.