ケーススタディ

大学の医療ネットワークがGigamonでランサムウェア攻撃を特定

過去6か月に発生したいくつかのインシデントは、攻撃者がサーバーの所有権を取得してから1時間以内に、迅速に捕捉することができました。被害が大きくなる前に、ぎりぎりのところで捕捉することができたのです。その理由は、私たちがセキュリティ・ツールを導入しており、Gigamonがすべてのデータをそれらのセキュリティ・ツールに供給しているからです。

KAJEEVAN RAJANAYAGAM氏

ユニバーシティ・ヘルス・ネットワーク サイバーセキュリティ担当ディレクター

課題

- East-Westトラフィックを可視化する
- セキュリティ・ツールへのトラフィック・データの供給
- リソースに制約のある公共部門の環境で動作

ソリューション

- GigaVUE® HCシリーズ
- GigaVUE TAシリーズ

顧客のメリット

- East-Westトラフィックの可視性を改善します
- ネットワーク接続を必要とする新しいセキュリティ・ツールの試験運用を容易にします
- スイッチの性能に影響を与えることなく、セキュリティ・ツールにデータを供給します
- トラフィックの重複を排除し、帯域幅の要件を低減することで、レガシー・ハードウェアの寿命を延ばします

お客様について

カナダのユニバーシティ・ヘルス・ネットワーク（UHN）は、主にオンタリオ州保健省が出資する公的医療機関です。トロントで、トロント大学と提携する4つの病院を経営しています。この組織はカナダ最大の病院ベースの研究プログラムで、心臓病学、移植、神経科学、腫瘍学、外科技術革新、感染症、ゲノム医学、リハビリテーションの分野で最先端の研究を行っています。

Kajeevan Rajanayagam氏はUHNのサイバーセキュリティ担当ディレクターです。8人から成るチームを監督しています。チームメンバーのうち3人はコンプライアンスに取り組んでおり、残りの5人はセキュリティ・ツールの技術的な導入と管理を担当しています。別のチームがネットワークを担当する一方で、彼のチームは、セキュリティの3つの主要分野である脆弱性管理、ネットワーク境界、エンドポイントを担当しています。Rajanayagam氏は、UHNのセキュリティ・スタックに含まれるすべての製品について、プライマリ・リソースとバックアップ・リソースの少なくとも2人のチームメンバーが、その製品の設定方法と、問題が発生した場合のトラブルシューティング方法を正確に把握するようにしています。

経営課題

多くの医療機関と同様、UHNは主にオンプレミス環境にあり、資産の98%を仮想マシン（VM）に、2%をパブリッククラウドに置いています。Rajanayagam氏は、クラウドに保存されている情報のほとんどは公開情報だと指摘します。

UHNが4年以上前にGigamonを購入した最初の理由は、ネットワークのEast-Westトラフィックの可視化など、可視化の必要性に対処するためでした。「セキュリティチームにとって最も重要なのは可視化です」とRajanayagam氏は断言します。「何かをいち早くキャッチできれば、それだけ早く事件を切り分け、損害の発生を防ぐことができます。」

ランサムウェアは、Rajanayagam氏にとって、そして医療分野全般にとって、特に差し迫った懸念事項です。「他の病院がランサムウェアに対処しているという記事を読むたびに、私たちが次の標的になるかもしれないと思っています」と彼は話します。

ネットワークの可視性を高めるため、チームはスパン・ポートを利用し、ForeScoutを使ってトラフィックとネットワーク・アクセスを監視するようになりました。しかしながら、それはインラインアプライアンスではないため、トラフィックの重複が発生してしまいます。チームは、インラインに設定されていないその他のセキュリティ・ツールも使用していました。彼らは、スイッチの性能に影響を与えることなく可視性を提供できるソリューションを必要としていました。

解決

Gigamonは、ArmisやForescoutといったさまざまなセキュリティ・ツールにデータを供給するために導入されました。最初のフェーズでは、GigaVUE-HC1アプライアンスがレガシー環境に追加されました。これらはトラフィックをコピーし、ツールに供給し、トラフィックの重複を排除します。次の導入フェーズでは、GigaVUE-HC3とGigaVUE-TA200を導入し、40GB、60GB、100GBというより高い帯域幅要件をサポートする予定です。

セットアップは驚くほど簡単でした。Rajanayagam氏によれば、アプライアンスを積み重ね、ラックに並べ、接続するのに1日、さらにそれらを設定し、すべてを稼働させるのに2〜3時間だったといいます。「ほとんど設定が要らず、すぐに使える状態でした。何もかも完了済みでした。既存のセキュリティ・ツールに手を加えたり、アップグレードしたりする必要はありませんでした。すべての作業はGigamon内で完結しました」と彼は断言します。

メリット

Rajanayagam氏は、Gigamonを使えば、新しいセキュリティ・ツールを簡単に試験導入できることを高く評価しています。Gigamonには常に2、3台のツールが接続されていますが、予備のポートがまだあるため、ネットワーク接続を必要とする新しいツールのためにトラフィックをコピーするのに使用できます。

彼が指摘するもうひとつのメリットは、Gigamonが既存製品の寿命を大幅に延ばしていることです。「コア・ネットワークをアップグレードしても、既存のハードウェア・アプライアンスのアップグレードを心配する必要はありません」と彼は断言します。それは、Gigamonが重複を取り除き、帯域幅を減少させることで、レガシー・アプライアンスでも同じデータ量を処理することができるからです。

セキュリティチームにとって最も重要なのは可視化です。何かをいち早くキャッチできれば、それだけ早く事件を切り分け、損害の発生を防ぐことができます。

KAJEEVAN RAJANAYAGAM氏

ユニバーシティ・ヘルス・ネットワーク サイバーセキュリティ担当ディレクター

次の段階では、Rajanayagam氏はGigamonのSSL復号化機能の使い方を探求する予定です。「それは2024年に私が集中したい優先事項のひとつです」と彼は言います。彼は、この機能がさまざまな形で価値をもたらすと予測しています。処理コストを削減し、復号化にかかる時間を短縮することができます。また、UNHのすべてのセキュリティ・ツールは、現在トラフィックの60〜70パーセントから見えない状態なので、その価値も高まるでしょう。

過去6か月間、Gigamonは、高額の損害を与える可能性のあるランサムウェア攻撃を特定するのに役立ちました。ある事件では、攻撃者がサーバーの所有権を奪いましたが、チームはその脅威を検知しました。Gigamon、Armis、Forescoutからのデータフィードにより、それぞれが実際の被害が出る前に事件を捕捉しました。

Rajanayagam氏によれば、攻撃は阻止されたため、そのような攻撃の潜在的なコストを数値化するのは難しいといいます。しかし、この事件が特定のランサムウェア攻撃者のパターンと一致したことから、ランサムウェア攻撃であっただろうと同氏は確信しています。幸いなことに、「1時間ほどで捕まえることができました」と彼は述べています。

ISAサイバーセキュリティについて

ISAサイバーセキュリティは、30年以上にわたり、ガバナンス、リスク、コンプライアンス戦略、アーキテクチャ＆エンジニアリング、アシュアランス、オフェンシブサイバーセキュリティサービス、マネージド＆ホスティングサービス、デジタルフォレンジック＆インシデントレスポンス管理の5つの主要業務において、サイバーサービスとソリューションを提供してきたIDC認定のフルサービスサイバーセキュリティ企業です。当社は最先端のテクノロジー・ソリューションと提携し、お客様がそのクライアント、スタッフ、そして一般の人々を安全かつ確実にサポートできるよう努めています。詳しくはisacybersecurity.comをご覧ください。

Gigamon について

Gigamonのディープオブザーバビリティパイプラインは、ネットワークレベルの実用的なインテリジェンスを活用し、お客様のオブザーバビリティツールを強化します。この強力なコンビネーションを活用すればIT組織は、セキュリティとコンプライアンスのガバナンスを維持しながら、パフォーマンスのボトルネックとなる根本原因をすばやく分析し、ハイブリッドおよびマルチクラウドのITインフラストラクチャ管理に伴う運用コストを削減できます。その結果、先進的な企業はクラウドへの完全な転換を実現できます。Gigamonは世界中で4,000社以上の顧客にサービスを提供しています。これにはFortune 100企業の80%以上、10大モバイルネットワークプロバイダーのうち9社、世界中の何百もの政府および教育機関が含まれます。詳しくは、gigamon.comをご覧ください。

Gigamon®

本社
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

11.23_01