Press Release
2022 年 3 月 22 日（火）
Gigamon Inc.

Gigamon Inc.　サイバー攻撃に対するクラウドアーキテクチャの強化方法を報告

ランサムウェアや DDos 攻撃に対する、クラウドアーキテクチャを理解しようとする際に必要な、分散、不変、および一時的という 3 つの属性に関する詳細を説明

2022 年 3 月 22 日（火）– “ビジビィリティファブリック”製品市場のグローバルリーダである Gigamon Inc.（本社：米国カリフォルニア州サンタクララ、日本代表：大久保 淳仁）は、サイバー攻撃に対するクラウドアーキテクチャの強化方法を発表しました。本レポートでは、クラウドアーキテクチャを理解しようとする際には、分散、不変、および一時的な 3 つの属性を念頭に置く必要があることに関する詳細を報告しています。

Simon Lee（Vice President, Asia Pacific and Japan）が it news ASIA 版に報告したレポートの抄訳版です。

パンデミックが発生し、多くの企業はクラウドへの移行を余儀なくされ、迅速に移行する必要がありました。

リモートオペレーション、テレワーク、およびリモートアクセスのインフラストラクチャに依存している現在、DDoS 攻撃者は新しい標的として、組織のテクノロジーインフラストラクチャのバックエンドを狙い始めました。

運用上の課題を克服するために、クラウドの採用は世界的に進められてきました。そのため、過去 24 か月でランサムウェアと DDoS 攻撃も急増し、今後 10 年間は続くと予想されています。

Radware の調査によると、2021 年の第 1 四半期に、ランサムウェアと DDoS 攻撃が 31%増加し、クラウドへの攻撃は全体の 92%以上、パケットのほぼ 84%を占めました。同様に、Check Point の調査では、世界のランサムウェア事例が 2020 年と比較し 2021 年の上半期だけで 2 倍になった事を報告しました。

ハイブリッド環境を利用する組織が直面する重要な課題の 1 つは、新しい脆弱性にさらされることではなく、サイバー攻撃に対する防御性です。

シンガポールでは、サイバーセキュリティエージェンシーが 2020 年にランサムウェア攻撃が前年の 2 倍以上になった事を報告しました。一例として、昨年 8 月、シンガポールの F＆B ビジネスのスタッフは、自社のサーバーとデバイス（クラウド内のものを含む）が、一般的なランサムウェアである NetWalker に感染していることを発見しました。同社は影響を受けたサーバーにもバックアップを保存していたため、データを回復することができませんでした。

このような例が増加しているため、私たちが注力しているのは破壊的なタイプの攻撃に対する回復力を構築することです。多くの組織は、これらのタイプの攻撃に対する回復力を実現するために、引き続きクラウドに注目します。しかし、これらのタイプの攻撃に対する回復力に役立つクラウドおよびクラウドネイティブアーキテクチャについてはどうでしょうか。

考えるべき 3 つの属性、分散、不変、および一時的：

- **分散 – アプリケーションとサービス**：アプリケーションが分散配信モデルを活用している場合（たとえば、コンテンツ配信ネットワーク（CDN）などのクラウドベースのサービスを活用している場合）、DDoS 攻撃は一方向に火力を集中させることで最も効果的に機能するため、心配する必要はありません。
- **不変 – データセット**：また、アプリケーションがレコードを変更せず、「書き込み時に追加」するソリューションを利用している場合（つまり、データセットが不変である場合）、そのデータの整合性に対する攻撃について心配する必要はありません。 このような攻撃を検出して表面化する方が簡単だからです。
- **一時的 – ワークロード**：そして最後に、アプリケーションが一時的なものである場合、攻撃者が永続性を確立して横方向に移動することについて心配する必要はありません。 また、そのアプリケーションインスタンスに関連付けられたトークンなどの機密情報の価値は、それらの資産が単に廃止され、新しい資産が比較的短い時間枠内でインスタンス化されるため、減少します。

したがって、分散型で不変で一時的な最新のクラウドネイティブアーキテクチャを活用することで、サイバーセキュリティの基本的なトライアド（3 要素）である機密性、整合性、可用性の問題に対処できます。

ペット対家畜

これにより、クラウドのコンテキストでしばらくの間話されてきた概念、つまりペットと家畜がもたらされます。ペットの名前はかわいいし、個別に認識できます。ペットが病気になった場合、飼い主は獣医に連れて行きます。飼い主は彼らに一生の思いやりを与え、ペットができるだけ長く健康的な生活を送るようにします。

従来のアプリケーションはペットのようなものです。各インスタンスは一意です。アプリケーションが感染した場合、それはサイバー獣医に運ばれます。「パッチインプレース」は、これらのインスタンスを一意にする従来のアプリケーションでは一般的です。 IT の仕事は、アプリケーションを可能な限り長く稼働させ続けることです。

一方、牛には名前がありません。 彼らの数はあいまいで、一般的に群れの牛を区別することはできず、彼らとの関係を築くこともありません。 牛が感染症などの病気になった場合は、群れを淘汰することになります。 最新のクラウドアプリケーションは牛のようなものです。 サービスの実行中のインスタンスを多数作成すると、各インスタンスは他のインスタンスと区別できなくなります。

牛が感染症などの病気になった場合は、群れを淘汰します。 最新のクラウドアプリケーションは牛のようなものです。 サービスの実行中のインスタンスを多数作成すると、各インスタンスは他のインスタンスと区別できなくなります。

- Simon Lee Vice President, Asia Pacific and Japan at Gigamon -

“サービスとしての「カオスエンジニアリング」”

クラウドは、このパラダイムに従うシステムの構築に役立つ多くのツールを提供します。 たとえば、Amazon は最近、サービスとしての「カオスエンジニアリング」を発表しました。これにより、組織は、実行中のインスタンスの停止など、本番ワークロードにカオスの要素を導入して、全体的なパフォーマンスに影響を与えず、ワークロードを超えないようにすることができます。 これらのタイプの運用上の後退に直面しても、回復力があるわけです。

このポイントに到達することは旅であり、それは複数のステップを経ることになります。 たとえば、組織は、アプリケーションのアーキテクチャを大幅に変更することなく、「ペット」（従来のアプリケーションとワークロード）をオンプレミスの世界からクラウドの世界に移動できます。

これの一般的な用語は「リフトアンドシフト」です。 アプリケーションがクラウドに組み込まれ、組織がクラウドネイティブツールに精通し始めたら、従来のアプリケーション（ペット）を、分散型で不変で一時的な（牛）の最新のアーキテクチャに再構築する作業を行うことができます。

言い換えれば、彼らはクラウド内のペットからクラウド内の牛に移動することができます。 ただし、組織は、この時点に到達した後、退行してペットの作成に戻らないようにする必要があります。 たとえば、パッチを適用したり、インスタンスを必要以上に長く稼働させたりすることはありません。

旅の各ステップでリアルタイムまたはほぼリアルタイムの可視性を維持することは、ペットまたはペットのような行動の早期発見を確実にするために重要です。 新しいワークロードがリフトアンドシフトモデルでクラウドに移行されるとき、またはワークロードが最新のマイクロサービスタイプのアーキテクチャに再構築されるときに、内部と外部の依存関係（つまり、ユーザーとアプリケーションの間の相互作用、および さまざまなアプリケーションコンポーネント自体の間）は、適切なポリシーを適用し、ペットの作成を検出してインセンティブをなくすために重要です。 これを行うには多くの方法がありますが、これらのアプリケーションのネットワークアクティビティのフットプリントを調べることで、これをマッピングするためのグラウンドゼロのアプローチが提供されます。

最終的に、クラウドの成果に向けた動きは、IT システムの効率を大幅に向上させることができます。 クラウドの復元力が適切に行われると、企業は新しいことをより迅速に実行できるだけでなく、どのような混乱が生じても、運用を継続的に維持できます。

英文のレポートは以下の it news ASIA 版よりご欄頂けます。
https://www.itnews.asia/news/ways-you-can-strengthen-your-cloud-architecture-against-cyber-attacks-573430

【Gigamon について】

Gigamon Inc. は、“ビジビィリティファブリック”製品市場 No.1 カンパニーです。全世界で販売パートナーおよびサービスプロバイダを通じて、4,000 社以上の企業へ、物理、仮想、クラウドネットワーク向けに可視化基盤ソリューションを提供しています。米国連邦政府機関のトップ 10 すべて、グローバル銀行トップ 10 の 7 行、Fortune100 企業の 83 社、モバイルネットワーク通信事業者トップ 10 の 8 社、テクノロジー企業トップ 10 の 8 社、医療関連プロバイダートップ 10 の 8 社に導入されています。Gigamon のミッションは、中堅・中小企業や分散拠点を持つ大企業や組織で、効率的運用かつ高 ROI のセキュリティ、監視システム環境を実現することです。本社を米国カリフォルニア州サンタクララに置き、世界 20 か国にオフィスを展開しています。

さらなる詳細情報、プロモーション活動、最新動向は https://www.gigamon.com/jp/をご覧下さい。

【本プレスリリースに関するお問合せ】
Gigamon Inc.
〒105-0022
東京都港区海岸 1-2-20
汐留ビルディング 3F
Sales 担当
Tel:03-6721-8349
Email： sales-japan@gigamon.com
URL： https://www.gigamon.com/jp/