2024 年 1 月 15 日

Press Release

アカマイ・テクノロジーズ合同会社

Akamai、クラウドとセキュリティにおけるトレンドを予測

オンラインライフの力となり、守るクラウド企業の Akamai Technologies, Inc.（NASDAQ：AKAM）は、クラウドとセキュリティにおけるトレンド予測を発表しました。

クラウド

- **マルチクラウドとハイブリッドクラウドの普及によって分散アーキテクチャが実現**

企業や組織はマルチクラウド／ハイブリッドクラウド戦略の領域に足を踏み入れ始め、さまざまなクラウドプロバイダーの優れたサービスをビジネスニーズに合わせてカスタマイズし、戦略的に取り込んでいます。

この傾向は 2024 年も続くと見られ、組織はクラウド支出に注目する一方で、アプリケーションのパフォーマンスと信頼性を高める取り組みに着手しています。このアプローチが成熟するにつれて、コストの最適化に加え、分散アーキテクチャの潜在能力を最大限に引き出す技術的および運用上のアジリティの獲得も可能になります。

分散コンピューティングの採用はまだ始まったばかりです。成功の鍵は分散データベースの普及にかかっています。これは開発者が革新的なアーキテクチャモデルを作成するための基盤になります。革新的なクラウドの普及だけでなく、アプリケーションやサービスの最適化とアーキテクチャの進化も実現します。

- **コンピューティングパフォーマンスに対して高まる要求**

アプリケーションのパフォーマンス要求の高まりに対応することは、現代の企業が熾烈な生存競争に勝ち残るうえで大きな課題となっています。これはユーザー体験が低品質であればビジネスに悪影響が生じるという懸念からくるものです。

現代の消費者は、非常にスムーズで応答性に優れたアプリケーションの操作感を期待し、時には強く要求しています。この点で後れを取ると、不満やブランドの信頼低下、売上減につながりかねません。

この課題は、2024 年により顕著になる可能性があります。事業者はデバイス間の相互接続の急増に対応しなければならず、満足のいくユーザー体験を提供するためには分散システム間でのリアルタイムのデータ交換が必要で、マシン間には信頼性と効率性に優れた通信が不可欠になるからです。

- **コンピューティングコストの課題に対処するための専門知識が直ちに必要**

クラウドインフラ／サービスへの移行を進めていくと、データストレージ、コンピューティング能力、エグレス（出方向の通信）帯域幅に関連する合計コストが急速に財源を圧迫して全体的な収益に影響を及ぼす可能性があります。

コンピューティングコストがもたらす喫緊の経済的な課題に加えて、ベンダーロックイン、特定クラウドプロバイダー／プロプライエタリテクノロジーへの依存、抽象化に関する懸念も、オルタナティブソリューションへの移行を困難にし、移行コストの大幅な増加や運用の中断を招く可能性があります。

こうした課題への対処には、クラウドテクノロジー、ソフトウェア開発、システム管理の専門知識が求められます。企業は、競争力のあるコスト構造を維持しながら最高のパフォーマンスを提供するために、アプリケーションを効果的に管理および最適化できるスキルを備えた人材を維持する必要があります。

セキュリティ

- **2024 年に AI を利用するランサムウェアが出現すると予測**

ランサムウェア攻撃は絶え間なく行われ、準備が整っていない組織に被害を与えます。こうした悪性行為のほとんどに関与しているのが、キルチェーンと呼ばれる一連の戦術と手法です。すでに、攻撃者は FraudGPT や WormGPT などのプログラムを通じて 生成 AI を攻撃に悪用しています。

2024 年は、攻撃に以下のような戦術がますます使用され、サイバー犯罪者と企業のどちらがより決定的な行動を取れるかが問われると予測されます。

1. 標的の優先順位付けや防御の回避といった困難なタスクを自動化し、ランサムウェア用の新たな武器を開発する。
2. 最適化された暗号化アルゴリズムにより、ランサムウェアの暗号化を強化し、復号やリバースエンジニアリングへの抵抗力を高める。
3. AI チャットボットを中心としたランサムウェアにより、被害者に対する攻撃のスケーラビリティと効率を向上させる。

組織にとって、取るべき行動は明確です。全体を可視化して、サイバー攻撃への耐性を強化します。また、すべてのアプリケーションアクセスを綿密に検証して、ゼロトラストのアクセスとセグメンテーションを実現します。

生成 AI を駆使するフィッシングツールは、より精巧なディープフェイクをさらに簡単に作成し、ソーシャルエンジニアリング攻撃をかつてないレベルに引き上げるでしょう。組織は、脅威の巧妙化を予測するだけでなく、組織の全体的なセキュリティおよびリスク対策を定期的に評価して、常に変化するサイバー脅威に対応する必要があります。

- **サイバーセキュリティが企業の戦略的優先事項となり、IT 部門だけが責任を負うものではなくなる**

サイバーセキュリティは、事後対応型から、より積極的なアプローチへと進化しています。企業がマルチクラウドプラットフォームやクラウドネイティブアプリケーションの導入を拡大するのに伴い、API のアタックサーフェスも拡大し、悪用されやすくなります。エッジコンピューティングは、攻撃対象になる可能性があり、激しいビジネスロジック攻撃に対して脆弱です。

特に公共部門機関は、個人情報保護の緊急性を強く認識しており、データ漏えいを最小限に抑えるためにゼロトラスト・アーキテクチャの導入が増えるでしょう。

また、組織はサプライチェーン保護にも重点を置く必要があります。サードパーティーベンダーからの信頼できる接続を悪用して境界の侵害を試みる攻撃者を阻止するためです。たとえば医療業界では、MRI 装置、インスリンポンプ、ウェアラブルデバイスといったネットワークに接続した医療機器の使用が拡大しており、医療サービス（遠隔医療や遠隔患者モニタリングなど）へのアクセスにおいて API が引き続き重要な役割を果たすでしょう。これが多数の脆弱性につながり、攻撃者に悪用されて、医療記録や患者データが狙われる可能性があります。

現在、多くの組織における API は事業部門ごとに開発が行われ、統一的なセキュリティ対策が十分ではない組織が見受けられます。増加する API 攻撃を防ぐため、組織は乱立するシャドウ API の把握、脆弱性対策、悪用防止へ包括的に取り組むことが有効な対策となります。
加えて、サードパーティ等の信頼できる接続を経由した侵害を防止するため、これまで手薄だった組織内部のセグメンテーションによるアクセス制御の強化が有望視されています。

Akamai Technologies について：
Akamai はオンラインライフの力となり、守っています。世界中の先進企業が Akamai を選び、安全なデジタル体験を構築して提供することで、毎日、世界中の人々の生活、仕事、娯楽をサポートしています。超分散型のエッジおよびクラウドプラットフォームである Akamai Connected Cloud は、アプリと体験をユーザーに近づけ、脅威を遠ざけます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、X (旧 Twitter) と LinkedIn で Akamai Technologies をフォローしてください。