2018 年 ホワイトペーパー

徹底的したセキュリティー: パブリック・クラウドを保護するための 5 つの検討事項

IT 設計者が抱えるパブリック・クラウドのセキュリティーに関する課題と対応策

IBM Cloud

IBM

情報テクノロジーの世界に肩を並べてやってきている 2 つの力。

まず、大規模なパブリック・クラウドの採用が加速度的に進んでおり、この流れはもう止めることはできません。また、データに対する脅威への心配と認識がグローバル規模で急速に高まっています。そのため、パブリック・クラウドのセキュリティーを疑問視する声があがっています。

その結果、IT 設計者はこう自問することになります「パブリック・クラウド計画を積極的に前進させながら、セキュリティー・リスクを軽減するにはどうしたらいいのか」と。

データはパブリック・クラウドへの関心をはっきりと示しています。McKinsey & Co.[1] のレポートは「パブリック・クラウドを使用すると、多くの会社が長年の間に築いてきた従来のサイバーセキュリティー・モデルが破壊される」と指摘しています。McKinsey が昨年実施した大企業 90 社の調査によると、80% の企業が2020 年までにパブリック・クラウドに重要なワークロードの 10% 以上を移行するか、現在のパブリック・クラウドの利用をすぐに倍増させる予定と答えています。意外なことではありませんが、同社は「重要なデータを保護するためには、サイバーセキュリティー・プラクティスを劇的に進化させて、パブリック・クラウド・サービスを利用すること」を企業に促しています。

セキュリティーの低さが招くコストの高さ

それと同時に、パブリック・クラウドのセキュリティー強化への取り組みは、非常に動的でグローバル規模の脅威へと突き進んでいます。IT 設計者は当然、インターネットを利用するアプリケーション、Web サイト、ワークロードに対して増大する一方の脅威の規模と範囲について警戒しています。非常に高度な技術を持ち、財源も豊富な攻撃者は、パブリック・クラウドとパブリック・アプリケーション・プログラミング・インターフェース (API) に脆弱性があると判断すると、それらの脆弱性を利用しようともくろみます。実際、そうしたもくろみは成功しています。1,000 社以上の企業を対象とした最近のある調査によると、76% が前年、2 回以上、分散サービス妨害 (DDoS) を受けたと報告しています。[2] 米国におけるデータ漏洩の平均コストは 700 万ドルに達し、DDoS 攻撃が成功した場合、毎時 250,000 ドルにも上ると見積もられています。

これからのセキュリティー対策

パブリック・クラウドがもたらすビジネスの大きなメリット、そしてサイバー攻撃者がアクセスを狙っているクラウド上の重要データへの潜在的な脅威は明らかです。パブリック・クラウドのセキュリティー・ソリューションを選ぶ際に、IT チーム、CTO、他のビジネス利害関係者がまっさきに考慮すべき 5 つの点をご紹介します。

1. ベアメタルを選択することで、環境を隔離する。

シングルテナントのベアメタル・サーバーは自社専有環境です。隔離された環境でワークロードを実行すると、ワークロードのセキュリティーがさらに強化されますが、セキュリティーの点から言うとそれぞれのコンピュート・サーバーによって対策は異なります。包括的なソリューションを実現するには、必ずシングルテナントの自社専用型ソリューションを選でようにしてください。一部のプロバイダーでは、ベアメタル・サーバーにハイパーバイザーを配置して仮想サーバーに変え、ワークロードを各種ユーザーに分配しています。自社ニーズに合ったソリューションを見つけましょう。

2. パブリック・クラウドのファイアウォールはどれも同じではない。

IT 設計者は、外部の脅威からの保護とコンプライアンス要件遵守の両方の面で、ファイアウォールがクラウド・インフラストラクチャーの保護において重要な部分を占めていることを理解しています。組織が従来のオンプレミス・アプライアンスからサービス型のソフトウェア・モデルに移行する中、適切なファイアウォールを配すれば、同じセキュリティー・レベルを両者に対して確実に維持できます。できるだけ多くのオプションを選べるソリューションを探すようにしましょう。たとえば、インスタンスレベルの保護、高可用性オプションとして展開可能なファイアウォールによるネットワークレベルの保護、単一のパブリック仮想 LAN 上のあらゆるサーバーの受信トラフィックを保護する専用ハードウェア・ファイアウォール、導入を容易にするポータルと API 双方のサポート、次世代の保護機能 (侵入防止システム、アンチウイルス、Web アプリケーション・ファイアウォール) などのオプションがあります。クラウドネイティブのファイアウォール・ソリューションは広く提供されていますが、物理アプライアンスも依然として企業にとって極めて重要です。セキュリティーとパフォーマンスを天秤にかけて選ぶ必要がないようにしたいものです。

3. セキュリティー・グループには多種多様なルールがある。

クラウド・セキュリティーの世界では、セキュリティー・グループは、ネットワーク・リソースへのアクセスを制御する役割を果たす IP フィルター・ルールのセットになります。これらのルールは、仮想サーバー・インスタンスのパブリック・インターフェースとプライベート・インターフェース双方での流入 (入口) トラフィックと送出 (出口) トラフィックの処理方法を決定します。セキュリティー・グループを単一または複数の仮想サーバー・インスタンスに割り当てられることは特筆すべき点です。利用可能なセキュリティー・グループで主要なネットワーク・セキュリティーの課題に適切に対処するようにしてください。たとえば、IT 設計者は通常、プロビジョニング直後から仮想サーバーを保護したいと思っています。そのため、仮想サーバーの注文時にセキュリティー・グループを確実に利用できるようにして、導入時にはサーバーを通過するトラフィックを完全にコントロールするようにしてください。また、ソリューション・プロバイダーのデータセンターで保護が必要なときに、すべての仮想サーバーに対してセキュリティー・グループが必要になる可能性が高いため、セキュリティー・グループ機能の使用に追加料金がかからないソリューションを見つけるようにしましょう。

4. 暗号鍵は成功への鍵。

調査に参加した 1,000 社のグローバル IT リーダーは、パブリック・クラウド・サービスを使用する意欲が高まる要因をリストから選択するように依頼されました。リストのトップには「暗号鍵をローカルに保存、管理する機能で自社データを暗号化する」が選ばれました。暗号鍵素材を安全に保護する改ざん防止ハードウェア・デバイスを特長としたクラウド・セキュリティー・ソリューションを見つけましょう。暗号鍵は必ず FIPS 140-2 Level 3 準拠ハードウェアに保存する必要があります。そのようなセキュリティー・モジュールを利用すれば、IT チームは暗号鍵をリモートで管理し、複数のアプリケーションやテナントで共有できるようになり、監査コストとコンプライアンス・コストを軽減できるはずです。また、SSL/TLS キーや大量のコード署名の保護のように、高いパフォーマンスが必要なケースでは、必ずそうした機能を提供できるハードウェア・モジュールを選んでください。

5. 操作を容易にしても、パフォーマンスやセキュリティーを低下させないこと。

IT チームでは、クラウド・セキュリティー・ソリューションを選ぶ際には、セキュリティーとパフォーマンスを天秤に掛けなければならないと嘆くことがよくあります。もう嘆くのはやめて、キャッシュやロード・バランシングなど、トラフィック最適化サービスと完全に統合した低遅延のセキュリティー・サービスを実現するソリューションを見つけましょう。使いやすさを重視したソリューションにより、大きな被害を生みかねない誤構成を防止するのと同時に、数分以内に Web アプリケーションと Web サイトを保護することができるでしょう。

パブリック・クラウドのセキュリティーを正す

パブリック・クラウド・プロバイダーを選ぶときには、セキュリティーを最重要視すべきです。Forbes によると、「ソフトウェアの専門知識とテクノロジーの大半をオンプレミスの世界からクラウドに変換することへの重点的な取り組みに成功」し、それを利用することで、競合他社を大きく引き離し続けるトップスリーのクラウド・サービス・プロバイダーが 1 社存在します。[3] そのプロバイダーは IBM です。IBM のパブリック・クラウドのお客様は、IBM Cloud セキュリティー・サービスの全機能にアクセスできるだけでなく、世界中数千社のお客様をサポートしている大規模なグローバル・セキュリティー・チームにもアクセスできます。

IBM のクラウド保護のアプローチは、最適な可視性を提供してパブリック・クラウド・サービスを先見的に監視すること、ユーザーによる脅威への迅速な対処を可能にすること、調査と軽減を格段に迅速化することに重点を置いています。IBM ソリューションでは、高度でありながら使いやすい分析のほか、保存中のデータと使用中のデータの両方をキー管理サービスで暗号化できます。また、ID およびアクセス管理機能も提供して、コンプライアンス管理を強化し、リスク全体を緩和します。

IBM のパブリック・クラウドの基本的なセキュリティー・ソリューションとサービスの一部をご紹介します。

ベアメタル・サーバー・ソリューション: 隔離した環境という形のセキュリティーに加えて包括的な制御と柔軟性のメリットを提供します。IBM Cloud ベアメタル・サーバーなら、コンピュート・リソースの他社との共有はなくなります。その代わりに、コンポーネントの構成とカスタマイズを含め、スタック全体を所有することになります。その結果、リソースを共有し、ワークロードを低下させる「厄介な隣人」について心配する必要はなくなります。

従来の環境から仮想環境へのシームレスな移行を実現するファイアウォール: IBM が提供する主要な機能の中でも、エンタープライズ向け最高級の、ハードウェアで加速化される高スループットのファイアウォール、FortiGate Security Appliance (FSA 10Gbps) があります。

クラウド・セキュリティー・グループ: 仮想サーバーをプロビジョニング直後から保護しながら、インスタンス・レベルでトラフィックをきめ細かく制御できます。

ハードウェア・セキュリティー・モジュール: 暗号鍵を改ざん防止/改ざんエビデンス・デバイス内で安全に管理、処理、保存することで、お客様の暗号化インフラストラクチャーを厳重に守ります。

クラウド・インターネット・サービス: ソフトウェア定義型セキュリティー・ソリューションにより、Web を使用するアプリケーションに対し、セキュリティー、回復力、パフォーマンス機能を提供します。数回のクリック操作またはシングル・ポータルや API 内からのコマンド実行により、より迅速でセキュアにインターネットを体験できます。

結論

今日のパブリック・クラウドは大体において、機密データを不要なリスクにさらさずに利用することが可能です。これでもかというくらい多くのパブリック・クラウド・サービスを提供する多くのサービス・プロバイダーがいる一方で、ユーザーはパブリック・クラウドに移行する前にこれらのサービスをじっくり調べて比較検討する必要があります。IBM Cloud は大手パブリック・クラウド・プロバイダー全社の中でも、企業セキュリティーの経験が最も豊富なグローバル・リーダーとして、お客様のビジネスが最も望んでいるもの、つまり、インフラストラクチャーの中心へのセキュリティーと安心感を提供するサービスとセキュリティー・チームを兼ね備えています。

詳細については、以下をご覧ください。
https://www.ibm.com/cloud/security

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America 2018

注記

1 “Making a Secure Transition to the Public Cloud” McKinsey & Co.、2018 年 1 月

2 “IBM Cloud Internet Services:Optimizing Security to Protect Your Web Applications” IBM、2018 年 2 月

3 “The Top 5 Cloud-Computing Vendors” Forbes、2017 年 11 月 7 日

TechTarget | Custom Media