クラウド セキュリティの発想

クラウド コンピューティングによって、企業の全体的なセキュリティ体制を強化することができます。とはいえ、セキュリティへのアプローチは大幅に変化しています。構成管理、パッチのコンプライアンス、マルウェア対策ソフトウェアの管理など、セキュリティ検疫に関する基本的な業務はこれまでどおり欠かせません。そのうえ、クラウドベースのインフラストラクチャやアプリケーションの管理には、新たなアプローチ、サービス、およびツールが必要になります。

そこで、Microsoft IT は、社内の迅速なイノベーションをサポートしながら、自社の IT インフラストラクチャの大半を Microsoft Azure に安全かつセキュアに移行させました。移行したアプリケーションとサービスは、自社を取り巻く環境全体で基幹業務の活動をサポートするものです。たとえば、ソース コードの管理のほか、財務、経営、対外、法務、人事、情報セキュリティといった部門のプロセスが含まれます。

イノベーションによって生じる課題

クラウド コンピューティング、モビリティ、モノのインターネットをはじめとする昨今のメガトレンドが、これらテクノロジを存分に活用する人々のイノベーションや競争上の優位性を後押ししています。各企業はこのようなイノベーションの多大な可能性を活かすべく先を争いつつも、プライベート クラウドとパブリック クラウドの両方で、無数のサービスやデバイスが急速に展開されていくなか、顧客データや知的財産を保護する必要に迫られています。いくつかのよく知られたセキュリティ侵害によって影響を受けた人々は、数百万人にも上ります。消費者と企業のどちらにとっても、サイバーセキュリティが新たなメガトレンドとなっていることは間違いありません。

このような前例のないテクノロジ イノベーションの発展を利用できる方法で組織の情報を適切に保護するには、これまでとは違うやり方で事を進める必要があります。情報セキュリティ、リスク管理、およびコンプライアンスの基本は変わりませんが、この新しい世界で企業がそれらを達成するには、従来の想定や関係、責任にとらわれない姿勢が必要となります。

新たな発想

マイクロソフトが自社の IT インフラストラクチャの大半をオンプレミスのデータセンターから Azure プラットフォームへと移行させるまでに、5 年かかりました。その取り組みのなかで、マイクロソフトは新たな発想を取り入れました。それは、インフラストラクチャ、アプリケーション展開、管理およびセキュリティ機能の民主化をサポートするものです。

多くの従来型の制御メカニズムはクラウドではもはや有効ではないばかりか、適用不能な場合もある、これに気付いたことが、重要な転機となりました。たとえば、クラウドではセルフサービスの購入モデルが採用されているため、運用環境への展開を許可する前にアプリケーションのセキュリティ レビューを行うことができなくなりました。ほかにも、Microsoft IT は、オンプレミスのときと同じ方法で物理ネットワーク トポロジを適用して、アプリケーションを監視しようと試みたこともありました。

クラウドでは、従来型のプロセスやソリューションは狙いどおりに機能しませんでした。アプリケーションは、アプリケーション セキュリティに対する承認がなくても、開発して展開できますが、従来のネットワークの構成概念をオンプレミスの場合と同様に展開することができず、数週間にわたってアプリケーションの展開が足止めされました。こうした例をはじめ多くの経験を通じて、マイクロソフトは、データセンターのようなクラウドを実現するよりも、クラウドのようなデータセンターを実現する方が容易だという結論に至りました。

クラウド コンピューティングとはパートナーシップである

Microsoft IT がクラウドで得た教訓は、管理責任とはサブスクライバーとクラウド サービス プロバイダー間のパートナーシップだけにとどまらないということです。それは、企業のセキュリティ組織とその DevOps (開発チームとオペレーション チーム) コミュニティ間のパートナーシップについても言えます。たとえば、Microsoft IT でこれまで厳しく管理していたホスト オペレーティング システムの物理インフラストラクチャの展開、パッチの適用、管理は、現在、ほかの担当者によって行われています。Microsoft IT 内では、各 DevOps チームが、アプリケーションやサービスのリリース ペースを決定すると共に、コンピューティング、ネットワーク、ストレージのリソースの構成と展開も行います。

クラウドへの移行戦略を成功させるには、適切な日々の責任をクラウド サービス プロバイダーに委任することが欠かせません。IT 部門は、パートナーシップの一翼を担うだけでなく、クラウド サービス プロバイダーにアカウンタビリティを割り当てる必要もあります。たとえば、Microsoft IT は、セキュリティ イベントに対する監視能力を速やかにクラウド規模へと拡大する必要があることに気付きました。一から始める代わりに、Microsoft IT では、グローバルな情報セキュリティを大規模に提供してきた長年の経験に基づくネイティブの Azure プラットフォーム サービスを利用しました。Advanced Threat Detection などの Azure サービスによって、セキュリティ侵害の指標を効果的に管理できます。侵害の指標とは、悪意のある活動の可能性を示すシステム ログやファイルに含まれるフォレンジック データです。これにより、セキュリティ イベント ストリーム内のデータの質が大幅に向上しました。

Protect (保護)、Detect (検出)、Respond (対応)

Microsoft IT にとって、クラウドへの移行における大きな変化は、"侵害を想定する" という概念でした。従来、アプリケーション開発ライフサイクルでのリソースの大部分は、アプリケーションのセキュリティ、ネットワークのセグメンテーション、ホストのセキュリティ強化といった予防的な活動に集中していました。今なお重要であるとはいえ、予防だけでは万全とは言えません。近年の大規模なセキュリティ侵害でも見られるように、高度な永続的脅威は現実のものであり、その結果、準備を怠った企業は深刻な影響を受ける可能性があります。

Microsoft IT は、攻撃者が侵入できるものと想定することで、攻撃が成功した場合に IT 部門が効果的な検出および対応機能によって影響を軽減できるようにする必要があることに気付きました。この想定では、すばやい検出と迅速な対応の実現に向け、取り組みと投資を強化する必要がありました。

この目標を達成すべく、Microsoft IT は 3 つの領域に投資しました。まず、インシデント対応チームと DevOps コミュニティがパートナーシップを開始しました。データの侵害が発生した場合に必要になる人員、プロセス、情報をこれらのチームが即座に特定し、設定するうえで、机上訓練が役立ちました。また、Microsoft IT では、Microsoft Power BI 用 Azure Security Center コンテンツ パックをはじめとするネイティブの Azure 機能を利用しました。コンテンツ パックによって、予期すべき内容、トリアージ方法、エスカレーションすべきタイミングを理解するためのトレーニングを両分野のチームに短時間で実施できました。最後に、Microsoft IT は、自動化に対してちょっとした投資を行いました。インシデント対応チームが必要とするユーザー特権や監査ログなどの適切なフォレンジック情報をすばやく収集するために、ネイティブの Azure API を使用しました。

DevOps チームがアプリケーションを制御

現在は、マイクロソフトの DevOps チームが、構成の管理、インフラストラクチャの監視、新たなレベルの問題およびインシデントの管理責任を担当し、Microsoft IT が管理とガバナンスの提供を担当するようになりました。Azure の特徴であるセルフサービスによって、マイクロソフトの DevOps チームは、アプリケーションを実行するインフラストラクチャの構成を含め、使用するアプリケーションを完全に制御しています。当然、このようなレベルのアクセスには、大きな責任とアカウンタビリティが伴います。

マイクロソフトは、Azure サブスクリプション アクセスのレビュー、Azure サービスの構成、パブリック エンドポイントの監査といった業務に関する運用上の期待事項についてチームの教育を行いました。これにより、セキュリティと運用の正常性を監視する目の数が、セキュリティ運用チームのほんの一部のメンバーから、Microsoft IT チームの全メンバーへと首尾良く増えました。

また、Application Insights や Azure Security Center など、監視と対応をサポートするツールが用意されているため、DevOps チームは、使用するアプリケーションのパフォーマンスとセキュリティの状態をリアルタイムで監視できるようになりました。これらのツールにより、アプリケーションに精通していない人々によって従来は処理されてきた部分において、パフォーマンス問題の早期検出、クラッシュの速やかな診断、すばやい応答が可能になりました。

さらに、セキュリティ チームも、Azure のアプリケーションやサービスに組み込むためのリスク管理ツールや自動化テクノロジを DevOps チームに提供しています。たとえば、IT 部門が開発した Azure Resource Management (ARM) のテンプレート、ARM ポリシーなどがあります。また、Azure の監査ログや、Azure SQL Database のログ、Azure Security Center を通過する情報をレビューする際に役立つ各種 Power BI コンテンツ パックなど、ネイティブの Azure 機能の利用も含まれます。目標は、セキュリティの制御とメカニズムを開発サイクルにまで絶えず押し上げることです。これにより、セキュリティ チームと DevOps チームの双方にメリットが生まれます。DevOps チームは、セキュリティ ツールおよびテクノロジを独自のアプリケーションに直接組み込んで改良する方法を学ぶと同時に、フィードバックをセキュリティ チームに提供して、セキュリティ チームがセキュリティ機能を継続的に強化できるよう支援します。

DevOps チームがアプリケーションの開発と管理を完全に制御しながらも、特定のセキュリティ業務をスキルの高い DevOps チームのメンバーに委託したことで、セキュリティ運用チームの予算を増やさずに、Microsoft IT のクラウド インフラストラクチャのセキュリティを向上させることができました。

ゲートではなくガードレール

過去 20 年間、従来型の IT 部門の業務では、プロセスベースのゲートを通じてデータセンターをセキュリティで保護することに重点が置かれてきました。変更管理が厳しく行われ、ソフトウェアのリリースはめったに行われませんでした。何よりも、企業とその製品およびサービスを攻撃しにくくしてインフラストラクチャを保護することの方が、オンプレミスの情報セキュリティ担当者の目標よりも優先されました。

一方、現在では、開発が加速され、アジャイルな業務と、クラウド上でいつでもアクセスできるイノベーションの利用によって実現されています。今や、クレジット カードがあれば、ネットワーク、ストレージ、コンピューティングのリソースを誰もが簡単に購入できるようになりました。アクセスはオープンで、いつでもどこからでも利用できます。従業員がリソースやサブスクリプションをそれぞれ会社名義で購入することもできます。こうした変化に伴い、アクセスを管理し、アプリケーションやサービスのセキュリティ体制、リスク、コンプライアンスを検証するための従来型のプロセスの多くは、効力を失いました。購入、変更管理、リリースといった活動を従来のゲート メカニズムに依存する方法は、もはや有効ではありません。

セキュリティ組織は、クラウドのセルフプロビジョニングの原則を踏まえ、変化する必要があります。クラウドでは、展開内容を把握すること、そのセキュリティ体制を評価すること、そして、適切に対応することが目標となります。幹線道路でガードレールによって車が崖下に落ちることがないようにするのと同じく、効果的なクラウド管理によって、イノベーションの促進に必要なリソースへのアクセスを実現しつつ、企業を確実に保護できるようになります。

Microsoft IT は、管理されていながらも、ほぼセルフサービスの環境をもたらします。クラウドのリソースは、Microsoft IT と Azure サブスクリプションの所有者間で協調的に管理されます。安全な展開を保証するために、Microsoft IT からビジネス オーナーと開発者のどちらにも ARM のテンプレートとポリシーが提供されます。また、DevOps コミュニティのメンバーに Azure サブスクリプションの所有権が付与されると共に、IT 部門には、Azure

RBAC の閲覧者ロールなど、各サブスクリプション内のすべてのアクティビティに対する可視性を提供するロールが割り当てられます。追加アクセスを必要とするイベントが発生すると、Just-In-Time アクセス プロセスが開始されます。Microsoft IT からは、Azure Security Center や Operations Management Suite などのサブスクリプション内で DevOps に最適化されたエクスペリエンスを有効するための構成や、その情報をデータ マイニングや機械学習用に中央データ リポジトリにフィードする処理の自動化を有効にするための構成に関するガイダンスが提供されます。

さらに、Microsoft IT は、検出および対応機能を実現するための監視サポートも提供します。ユーザー アクセスのレビュー、エンドポイントの検証、運用ログのレビューといったサブスクリプション監査機能によって、Microsoft IT とサブスクライバーの両者が、展開した Azure リソース、セキュリティ イベント、および構成の変更を監視できるようになります。

承認されたシャドウ IT

マイクロソフトの従来型のオンプレミス環境では、ネットワーク サービスやコンピューティング サービスの購入に多くのリソースと時間がかかる状況が、迅速な開発への強いニーズと結び付き、監視の届かない "シャドウ IT" を生み出しました。Microsoft IT が急速に変化するビジネス ニーズに合わせて常に迅速に対応できるとは限らなかったため、一部のアプリケーションやサービスが Microsoft IT の監視の目を逃れて作成されるようになりました。その結果、環境のインベントリ作成だけでなく、そこで保存/処理されるデータの適切な保護も難しくなり、監視や管理の行き届かない、並行したコンピューティング インフラストラクチャに関するリスクが生じました。そこで、Microsoft IT は、この問題に対する新たなアプローチを取ることにしたわけです。

予防面では、Microsoft IT は、展開テンプレートや ARM ポリシーを作成したほか、ネイティブの Azure API を使用した自動化機能を開発して、企業データに適切な保護が適用されるようにしました。また、IT 部門の管理下にないサブスクリプションやワークロードを特定し、共同管理できる検出機能も作成しました。IT 部門内のほとんどのサブスクリプションは共同管理されていますが、ときどき IT 部門の管理外で作成されるものがあるためです。Azure では、展開または使用されたリソースごとにコストがかかります。コストは請求明細書で示され、明細書は Azure アカウント センターから確認することも、REST API からプログラムによってアクセスすることも可能です。そのため、Microsoft IT は、使用されている Azure サブスクリプションを確実に確認できます。現在、IT 部門によって、共同管理されているサブスクリプションと有効なサブスクリプションの簡単な比較が行われています。有効な、かつ共同管理されていないサブスクリプションは、すばやく特定され、共同管理下に置かれます。

Azure はほぼセルフサービスであり、既にリスクおよびセキュリティに関する厳格な標準に準拠しているため、グループが企業の信頼境界の外でイノベーションを生み出す必要がなくなります。前述の ARM の展開テンプレートとポリシーを通じて、IT 部門は、DevOps が会社をリスクにさらすのを防ぐために必要なガードレールを提供できます。また、Azure によって、マイクロソフトは、承認されたシャドウ IT を受け入れ、推進することさえできます。これは、Microsoft IT が従来型の IT 制御ではなく、オペレーショナル エクセレンスと動作に基づく業務に対してより重点を置くようになったためです。

基本を押さえる

これらのさまざまな変化にかかわらず、Microsoft IT のセキュリティ運用チームは、今後も保護、検出、対応に役立つ機能を提供します。インフラストラクチャとアプリケーションのセキュリティ検疫の重要性は、オンプレミスのアプリケーションとサービスを Azure に移行しても変わらないばかりか、より一層高まることでしょう。マイクロソフトは、正常な環境を維持するために、ウイルス対策用のソフトウェアとパッチの慎重な適用、脆弱性の管理、SSL の利用、保存データの暗号化、監査ログのレビュー、構成の管理といった取り組みを継続する必要があります。

Microsoft IT は、検疫機能をさらに強化しました。マイクロソフトでは、責任とアカウンタビリティを DevOps チームに移行するだけでなく、新しい Azure の機能とサービスを利用しました。Azure Security Center、ロールベースのアクセス制御、ARM 展開テンプレート、Azure SQL Database の脅威防止機能、オンプレミスのセキュリティ イベント監視機能との統合などは、侵入防止手法であり、効果的な検出と対応手段を提供します。

クラウド パートナーシップによってセキュリティ チームと開発者の双方がメリットを得ることができます。マイクロソフトでは、セキュリティと迅速なイノベーションのバランスを保つために、各チームが密接に連携しています。このモデルでは、クラウド サービス プロバイダーと DevOps チーム間でセキュリティ上の責任が連携されるため、インフラストラクチャの検疫、アプリケーションのセキュリティ業務、およびオペレーショナル エクセレンスが、これまで以上に重要になります。

まとめ

本稿では、Microsoft IT と Microsoft Azure のコンテキストにおいて、クラウドを使用してセキュリティ機能の民主化と分散化を行う方法を説明しました。次の表は、一般的なセキュリティ機能とマイクロソフトでの実現方法を示しています。

表 1. セキュリティ機能

セキュリティ機能	機能またはソリューション
イベントの監視とポリシーの管理	Azure Security Center
ハイブリッド クラウドの管理と保護	OMS
ID 管理と認証	Azure Active Directory と Azure Multi-Factor Authentication
保存データの暗号化	Azure SQL Database Transparent Data Encryption Azure ドライブ暗号化
シークレットとキーの管理	Azure Key Vault サービス
最小特権アクセス	Azure RBAC
高度な脅威保護	Azure SQL Database Threat Detection

詳細情報

Microsoft IT Showcase (英語)

microsoft.com/ITShowcase

Microsoft Azure

https://azure.microsoft.com/ja-jp/

Microsoft Azure セキュリティ センター

azure.microsoft.com/ja-jp/support/trust-center/