ORACLE
CLOUD

共有責任モデルの理解

クラウド・サービスを使用する企業のセキュリティ上の義務

ORACLE WHITE PAPER | 2017 年 1 月

ORACLE

はじめに

クラウドを採用することで、柔軟性の向上と大幅なコスト削減というメリットが見込まれます。そのため、ビジネスクリティカルなアプリケーションをクラウドに移行することは、どのような規模の企業でもますます優先度の高い課題となっています。250,000人以上の情報セキュリティ担当者を対象に行われた最近の調査では、77%以上の企業がすでにクラウド・サービスを採用しており、クラウド・サービスを使用している企業の10%がヘビー・ユーザーを自認していることが判明しました。

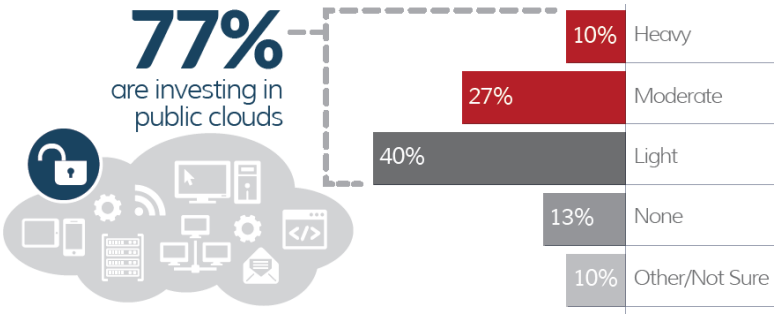

図1.ますます多くの企業がパブリック・クラウドのアプリケーションを使用しています。

多くの企業が定期的に新しいアプリケーションを採用しているものの、クラウド・サービスのセキュアな採用を実際に経験している企業はほとんどありません。企業のビジネスクリティカルなニーズをクラウドに移行する場合、どのような単一ソフトウェアのアップグレードよりもはるかに大きな影響を及ぼします。クラウドの採用は必ずと言っていいほど、事業運営の新たな枠組みとなる全社規模のイニシアチブの一環として行われます。そのための高い重要性と期待度を受け、企業は相当の時間とリソースを費やして、機能や冗長性、グローバル・インフラストラクチャ、サービス・レベル合意(SLA)といったクラウド・サービスのあらゆる側面を評価します。しかし、クラウド・サービス・プロバイダ(CSP)のサービス利用条件文書のある項目は繰り返し見過ごされます。それは共有責任モデルです。

共有責任モデルは、MicrosoftからAmazonまで、すべてのCSPのサービス利用条件文書で詳しく説明されています。それにもかかわらず、理解されずに誤解されることが最も多い概念であることはほぼ間違いありません。簡単に言えば、共有責任モデルとは、CSPがセキュアで常に利用可能なサービスを維持する責任と、企業がサービスのセキュアな使用を保証する責任を概説したものです。このような概念を理解するのが難しく、様々な解釈を生みやすいのはなぜでしょうか。*サービスのセキュリティ*と*サービスのセキュアな使用*には大きな違いがあるのでしょうか。クラウドに移行しない企業はこの種の責任に対処する必要はないのでしょうか。

このホワイト・ペーパーでは、混乱の背後にある根本原因と、混乱の結果の不運な事例について考察するとともに、企業がどのような方法で共有責任モデルに対応し、共有責任モデルを受け入れて、成功を収めているかを紹介します。

共有責任モデルとは、クラウド・サービス・プロバイダがセキュアで常に利用可能なサービスを維持する責任と、企業がサービスのセキュアな使用を保証する責任を概説したものです。

クラウド・サービスのセキュリティ・インフラストラクチャに関する誤解

共有責任モデルをめぐる誤解の多くは、先入観と従来のソフトウェア・モデルにおける過去の経験から生まれています。製品としてMicrosoft Officeスイートを例に取ってみましょう。大まかに言って、従来のMicrosoft Exchange電子メールをデプロイするには次のことが必要です。

» 従業員/ユーザー情報用のActive Directoryと統合する
» 実際のWindowsまたはメールボックス・サーバーをインストールする
» エッジ・トランスポート・サーバーをインストールしてスパム・フィルタリングとメール・フローを処理する
» Outlook電子メール・クライアントをPCとラップトップにデプロイする

デプロイするサーバーやクライアントがないため、企業は、Exchangeをクラウドに移行する際に必要なのは次のことだけだと誤解します。

» オンプレミスのActive Directoryをクラウド・サービスと統合する
» スパム・フィルタリングやその他のメール・フローをクラウド・サービスで構成する

従来のExchangeアプリケーションが依存しているすべてのオンプレミスのセキュリティ対策は見逃しています。ファイアウォールは、特定の場所(通商禁止国など)からのログインをブロックするように構成されています。侵入防止システムにより、疑わしいIPアドレスや悪意があることが判明しているIPアドレスからのログインがブロックされます。行動分析プラットフォームにより、侵害された資格証明を使用した内部関係者による脅威や攻撃が検知されます。セキュリティ情報およびイベント管理(SIEM)ソリューションやログ管理ソリューションにより、重要な構成の変更に関するアラートが管理者に送信されます。こうしたセキュリティ対策やそれ以外のセキュリティ対策により、企業の構内にあるアプリケーションはすべて保護されているため、ある特定のアプリケーションについても当然セキュリティ対策が取られているものと考えてしまうことが多いのです。ここに例として挙げたセキュリティ対策は、サービスのセキュアな使用を保証するために必要です。したがって、これらをインストールして維持する責任は100%企業側にあります。

「一度設定したらメンテナンスは不要」という神話

クラウド・アプリケーションの採用に向けて準備する際に、多くの企業は、労力とリソースの大部分が初期オンボーディング・プロセスで必要になるものと想定してITリソースをプランニングします。きちんとしたガイドラインに従って各種サービス設定を構成すれば、継続的なメンテナンスに必要なリソースは大幅に減少するだろうというのが多くの企業の考えです。結局のところ、ITスタッフは初期設定の一環としてクラウド・サービスの経験を積み、使い方に慣れるはずだからというわけです。残念ながら、このようなことは現実のデプロイメントには当てはまりません。企業が共有責任モデルの役割を果たせない最も一般的な理由の1つがこの考え方です。

クラウド・サービス採用の初期段階で、IT管理者は、サービスの主要な構成設定などの様々な要素からなるロールアウト・プランを定義します。この設定には、資格証明の複雑さやローテーションなど、ユーザー固有のセキュリティ要件が含まれています。また、ユーザーと管理者の権限設定も含まれています。この権限設定により、どのユーザーがどのアプリケーションへのアクセス権を持つか、どの管理者が新規ユーザーの作成や既存の権限の変更を行えるかを識別します。こうした設定は、当初は明確に定義されていますが、企業がビジネス全体をよ

り適切にサポートしようとする中で自然とずれていきます。さらに、調整を元の設定に戻さなければ、一時的な変更が永続化されてしまいます。

IT管理者は構成のずれがないか定期的にチェックすることが可能であり、チェックするべきですが、必要なリソース量の問題から、そのような作業が熱心に行われることはめったにありません。たとえば、すでに退職している管理者によって6か月前に構成が変更された理由を追いかけようとすると非常に時間がかかります。残念ながら、徹底的な調査を行わずに構成を単に元に戻すという選択肢はありません。多くのIT管理者が証言してくれるでしょうが、そのような行動を取れば、大抵は、翌日の取締役会で必要になる重要なデータにアクセスできないことを知った役員が怒って夜遅くに電話をかけてくる結果になります。

そのため、多くのIT管理者は「壊れていないかぎりは直さない」モデルにただ従っているのです。構成のずれのチェックを四半期ごとの監査作業まで延期する企業もありますが、一般的なのは、単にインシデントへの対応として設定を修正するのを待つことです。残念ながら、どちらのアプローチも構成のずれにつながるため、企業は攻撃に対して脆弱な状態のまま、多額の金銭的負担を強いられることになります。

責任を果たさなかった場合

どのようなセキュリティ対策を取る必要があるかを企業が明確に理解せず、構成のずれを最小限に抑えることができないと、多くの場合、重大な影響が生じます。企業の可視性とセキュリティの不備から悲惨な結果に至った実例が数多くあります。

不満を持つ従業員が原因で企業が数百万ドルを失う

業種	製造
インシデントの時期	2015年
クラウド・サービスの使用状況	この企業は、社内アプリケーションの多くをパートナ向けのアプリケーションとともにクラウドに移行した。
インシデントの詳細	不満を持つ従業員が辞職前に数十のAmazon Web Service (AWS)インスタンスを開始した。
インシデント発見の経緯	Amazonから多額の請求書が届いて初めて、この企業はインシデントに気付いた。
共有責任モデルにおける義務	AWSインスタンスを開始したユーザーは、有効な特権ユーザーだった。しかし、この企業には、複数のAWSインスタンスの開始といった異常なアクティビティを検知して警告する自動化システムがなかった。
インシデントの影響	総額は公表されなかったが、数百万USドルと推定される。
インシデントへの対応	インシデントの後、この企業はクラウド・セキュリティ・ソリューションをデプロイした。このソリューションは、自動的にクラウドのセキュリティ設定を監視し、新しいAWSインスタンスの開始といったアクティビティについて警告するなど、様々な機能を備えている。

企業がランサム攻撃の後、営業を停止

業種	ホスティング・プロバイダ
インシデントの時期	2014年
クラウド・サービスの使用状況	この企業は、クラウド・サービスを利用してビジネス・モデルの根幹をなす顧客データをホスティングしていた。
インシデントの詳細	特権ユーザーに対するフィッシング攻撃により、ハッカーがAWS資格証明へのアクセス権を得た。特権アクセスを手に入れた後、ハッカーはクラウド環境のコントロールと引き換えに身代金を要求した。
インシデント発見の経緯	この企業が分散型サービス拒否(DDoS)攻撃について調査している最中に、ハッカーによって故意に残された身代金要求をITグループが発見し、攻撃の正体が判明した。
共有責任モデルにおける義務	この企業は、最初のフィッシング攻撃を阻止するのに十分なセキュリティを欠いていた。しかし、さらに重要なのは、資格証明が侵害されたことやバックアップの管理者ユーザーが作成されたことを示す疑わしい行為を検知するための自動化ツールがなかったことである。
インシデントの影響	この企業がクラウド・サービスのコントロールを取り戻そうとすると、ハッカーはバックアップの管理者アカウントを使用してクラウド・サービスからデータをすべて削除した。
インシデントへの対応	攻撃の重大性により、この企業は数日のうちに営業を停止して廃業した。

医療機関がHIPAA違反により罰金を課せられる

業種	ヘルスケア
インシデントの時期	2014年
クラウド・サービスの使用状況	医療機関がクラウド・サービスを生産性スイートとして採用した。
インシデントの詳細	間違った構成が原因で、個人健康情報(PHI)が外部に送信されないようにするためのチェックを電子メール・ソリューションがバイパスした。
インシデント発見の経緯	四半期ごとの構成監査の後にようやくミスが発見された。発見後、この医療機関はインシデントを速やかに報告した。
共有責任モデルにおける義務	この医療機関には、重要な構成設定が変更されたときにIT担当者に通知する自動アラートがなかった。
インシデントの影響	財務面の影響はまだ確認中だが、最大で150万USドル程度の罰金が予想される。
インシデントへの対応	インシデントの後、この医療機関は、重要な構成変更についてのリアルタイム・アラートをITスタッフに自動的に送信するクラウド・セキュリティ・ソリューションをデプロイした。

以上の例に示したように、共有責任モデルをめぐる誤解から生じたセキュリティ・ギャップは、悲惨な結果につながっています。多くの企業が多大な財務損失を被っており、営業を停止した企業さえあります。幸運にも、企業はこうした事例から学習することで、共有責任モデルにおける自らの役割をより的確に果たすとともに、クラウドのセキュリティ体制全体を改善しつつあります。

共有責任モデルのもう1つの側面

共有責任モデルは、必要なセキュリティ対策の大部分を企業が負わされる不公平な仕組みのように思えるかもしれません。マスコミを賑わすような一部のインシデントほどセンセーショナルには扱われないものの、クラウド・サービス・プロバイダが共有責任モデルにおける役割を果たすべく対応した実例がいくつかあります。

ハッカーがGOOGLE APPSを使用して攻撃を仕掛ける

影響を受けたサービス	Google Apps
インシデントの時期	2015年
インシデントの詳細	ハッカーがGoogle Apps (具体的にはGoogleドライブ)を使用してフィッシング攻撃を仕掛けた。ハッカーは、Googleドキュメント上に偽のログイン・ページを作成し、それを使用してログイン資格証明を取得した。偽のログイン・ページは、google URL (google.com/…)が使用されていることも含めて、本物のように見えた。
インシデント発見の経緯	攻撃は、Googleがセキュリティ・ベンダーから警告されるまで、気付かれることなく続いた。
共有責任モデルにおける義務	技術的に見れば、この攻撃はGoogle Appsサービスの可用性やセキュリティに影響を与えなかったので、共有責任モデルに不備があったわけではない。それでもGoogleは、自社のインフラストラクチャが悪意をもって使用されていないことを保証するとともにサービスへの全面的な信頼を回復するために、迅速に対応しなければならなかった。

OFFICE 365で従来の脆弱性が発見される

影響を受けたサービス	Microsoft Office 365
インシデントの時期	2013年および2014年
脆弱性の詳細	Microsoft Office 365のクロス・サイト・スクリプティング(XSS)脆弱性により、社内のどのユーザーでも企業Office 365環境に対する完全な管理権限を得ることができた。
脆弱性発見の経緯	この脆弱性は、Office 365の報告企業によって監査中に初めて発見された。
共有責任モデルにおける義務	脆弱性があることを知らされたMicrosoftは、2か月以内に問題を修正した。Microsoftは、製品の脆弱性が利用されないうちに対処することを目標に掲げ、製品の脆弱性を発見するよう促している。これは同社の標準的なビジネス・プラクティスであり、Microsoftが共有責任モデルにおける義務を果たしているいくつかの方法の1つである。

共有責任モデルへの対応

企業は、クラウド・サービスのセキュアな使用を保証し、共有責任モデルにおける義務を果たすために、新たなアプローチを取る必要があります。ファイアウォールやプロキシ、その他のソリューションを利用してエンタープライズ・ネットワークの周囲を保護するという従来のアプローチは、クラウド・サービスには通用しません。また、サービスの初期構成のみに注目し、構成のずれや変更が発生しても同じレベルのセキュリティを期待するのは現実的でないことも実証されています。企業が従来のアプローチの限界を認識していたとしても、ソリューションが明らかなことはなかなかないのが残念な点です。

IT予算には常に厳しい目が注がれており、企業がクラウド・サービスを採用する場合は特にその傾向が強まります。事実、IT支出削減の可能性は、クラウド・サービス採用のメリットとしてよく期待されることの1つです。このような状況を考えると、企業が共有責任モデルにおける役割を果たすためのリソースは不足している場合がほとんどです。クラウド・サービス構成の手動監査を定期的に行う専任のリソースが不足していることは間違いありません。

企業は、自力では埋められないギャップを埋めるために、クラウドベースのセキュリティ自動化サービスに頼ろうとしています。こうしたソリューションは、Microsoft Office 365、Google Apps、AWS、Boxなどのビジネスクリティカルなサービスと緊密に一体化されており、重要な構成変更について企業に警告します。構成を自動的に元に戻すことが可能な場合もあります。こうしたソリューションでは、ユーザーの行動分析により、侵害された資格証明や、攻撃を示す危険な行動あるいは異常な行動を特定することもできます。

クラウド・セキュリティの自動化は、企業のクラウド・サービス採用が加速し続ける中で待ち望まれていた、共有責任モデルに対応するソリューションです。

Oracle CASB Cloud Serviceについて

Oracle CASB Cloud Serviceは、クラウド・フットプリント全体を保護するための革新的なアプローチをもたらします。APIベースのクラウド・アクセス・セキュリティ・ブローカ(CASB)のパイオニアであるOracle CASB Cloud Serviceは、Software-as-a-Service (SaaS)、Infrastructure-as-a-Service (IaaS)およびPlatform-as-a-Service (PaaS)の環境に可視性とセキュリティを提供する唯一のソリューションです。

ORACLE

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

Integrated Cloud Applications & Platform Services

Making Sense of the Shared Responsibility Model
2017 年 1 月