



メールフィルタでは不十分

狙われるクラウドメールに、必要な防御策とは？

メール環境を「Office 365」や「G Suite」といったクラウドメールサービスへ移行する企業が増えています。自社でメールサーバーやシステムを管理する必要がない上、外出先からスマートデバイスでアクセスが可能となるため働き方改革の推進にも有効とされています。しかしクラウドメールを標的としたマルウェアなど攻撃の手口も巧妙化しています。クラウドメールには「多段・多層」でのセキュリティ対策が不可欠になっています。

リモートワークやファイル共有、便利さの裏にあるリスク

企業がメール環境を移行する際に利用しているクラウドメールは、SaaS (Software as a Service : サービスとしてのソフトウェア) と呼ばれるサービスに分類されます。代表的なものとしては「Office 365」や「G Suite」などがあります。それらのクラウドメールはマルチデバイス対応のため、社内外のPCあるいはスマートデバイスから、最新の状態に同期されたメール環境へアクセスできます。サービスによってはクラウド上でファイルを共有する機能も備えているなど、場所を選ばず社内同様の業務環境を整えられるため、クラウドメールはリモートワークに最適なツールのひとつといえます。メールサーバーが外部にあるため、メール保管用ストレージの残量に頭を悩ませるなど運用・管理の負担軽減というメリットもあります。

しかし、オンプレミスと同様、クラウドメールもインターネットを介しているため、マルウェア感染などのリスクがあります。サービス側でもスパムメールやマルウェアなどのフィルタリング機能を提供していますが、巧妙化する標的メールや未知のプログラムで動くマルウェアや不正アプリなどはそれらをすり抜けることもあり、万全とは言えません。

ファイル共有機能にもリスクが潜んでいます。例えば、ある端末からウィルス感染したファイルをアップロードした場合、それにアクセスした社内・関係者にも感染が拡大します。もしファイルに個人情報などの機密情報が含まれていたら、情報漏えいに発展することもあります。企業はクラウドメールの利便性と表裏一体である、セキュリティリスクへの管理・対策も念頭に置く必要があります。

クラウドメールにこそ、多段・多層防御が必要

クラウドメールは、社内PCに加えて、スマートフォンやタブレットなどからの社外アクセスもあり、スマートデバイスで使用されるSNSやアプリケーションなども攻撃の標的となります。そのため、複数ポイントでセキュリティ対策を行う多段・多層防御が不可欠です。例えばメールが侵入する経路では、ゲートウェイとエンドポイントのそれぞれでマルウェア対策を行います。最近では危険なものか安全なものかの判断が難しい“グレーな添付ファイル”が増えているので、グレーなファイルを仮想環境で実際に実行させてチェックする「サンドボックス」が有効です。これらの対策と「Office 365」や「G Suite」などのクラウドメールサービスを組み合わせた対策も一般的になっています。

例えば、NTT Comが提供する「Cloud App Security」は、Office 365に標準装備されているセキュリティ機能を強化するサービスです。Office 365のスパムメールやマルウェアをフィルタリングする機能(Exchange Online Protection)と連携し、未知の不正プログラムなどに対してサンドボックスやWebレピュテーションなどの機能で強化することで、多段・多層防御を構築。その結果「Cloud App Security」は、2017年にOffice 365のセキュリティ機能をすり抜けたマルウェアやランサムウェア、フィッシングメールなどを全世界で約349万件、検知した実績があります。また、Office 365では対象外だった内部メールや、Exchange Onlineでの送受信ファイル、OneDrive for Businessのファイルもスキャンするため、共有ファイルを通じた内部感染の拡大も防ぎます。

特徴は、導入が簡単スピーディーという点です。Office 365とAPI連携するため、DNS(Domain Name System)の切り替えやメール経路などの変更も不要。送信先をアプライアンス機器に変更するソリューションで起こり得る、メール送受信の遅延などありません。Active Directoryとも連動してユーザー管理の自動化も可能なので、マルチデバイスの管理もしやすくなります。適用範囲もユーザー単位で広げられるため、例えば部署、プロジェクト単位などといった柔軟な導入・利用もできます。

「Cloud App Security」は、Office 365にアドオン機能を追加するような感覚で、セキュリティ対策の多段・多層防御を可能とするサービスといえます。攻撃メールの量がそのままであってもそれらがユーザーにまで届いてしまうケースは大幅に減るため、情報システム部門が事後対応に追われる負担の軽減にもつながります。

関連サービス

Cloud App Security

Office 365 標準セキュリティを強力にカバーするクラウド型セキュリティサービスです。

社外に置かれるメールやクラウド共有ストレージデータのセキュリティを補完し、クラウドサービスを安心してご使用いただくための新しいソリューションをご提供します。

メールセキュリティ

ウイルスチェック機能と迷惑メールフィルタリング機能をセットで提供する、「Biz メール&ウェブ ビジネス」のオプションサービスです。

ウイルスメールや迷惑メール、フィッシングなどに対する最新のメールセキュリティ対策が可能となります。

テレワーク・スタートパック

ノートPCとモバイル通信、セキュリティサービスをパッケージ化したサービスです。アンチウイルスソフトやファイアウォールから不正プログラムの実行阻止までテレワークを始めるためのセキュリティ対策が設定されたPCを納品します。面倒な設定作業が不要なので、最短10分でPCをご利用できます。