セキュリティ対策虎の巻（第2回）

攻撃を食い止める多層防御。UTMソリューション

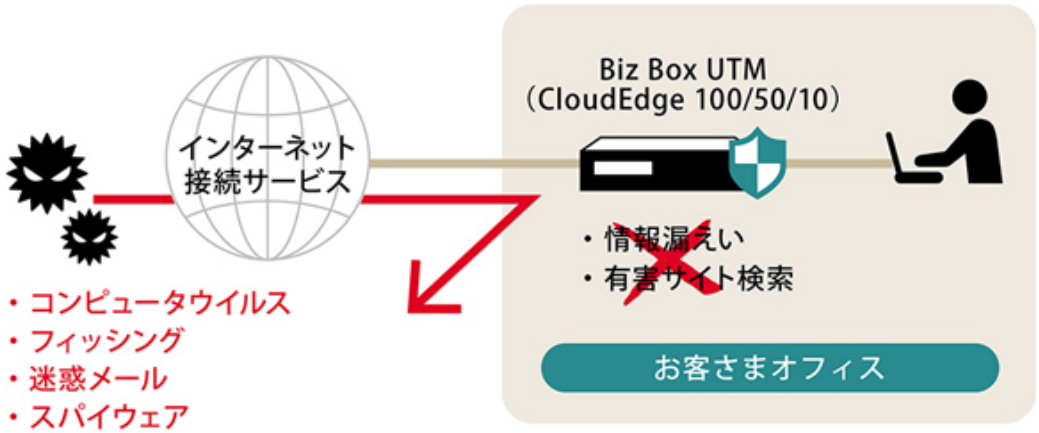
2020.11.04

よくマスコミで報道される企業の情報漏えい事件の多くは、セキュリティ対策をしていなかったわけではない。攻撃者の手口の巧妙化が進むと、これまでは有効とされていた対策が通用しなくなるからだ。ウイルス対策ソフトやファイアウォールだけといった、単一的・局所的なセキュリティ対策ではもはや防ぎ切れなくなっている。

こうした課題を解決する1つの方法が多層防御だ。攻撃の入り口から出口まで、複数のセキュリティ対策を組み合わせて“どこか”で攻撃を食い止めるやり方だ。これを実現するのがUTM（統合脅威管理）である。

UTMは複数のセキュリティ機能を1台に統合し、さまざまな脅威に対応できる。NTT西日本では、中小規模の事業所に適したソリューションとして「セキュリティおまかせプラン プライム」を用意している。このソリューションは、ネットワークの入り口と出口対策に加えて、24時間365日の通信監視や標的型攻撃メール対策訓練を含む、いわば“セキュリティのよろずおまかせ”プランでUTMソリューションも組み込まれている。悪意のあるメールやウイルスといった外部脅威への防御と、メール訓練機能による社員のセキュリティ意識向上および社内の感染拡大を未然に防ぐ内部脅威への防御を備えた「事前対策」。さらに、万が一の異常発生時には電話やメールお知らせをする「事後対策」により、セキュリティ対策を複合的にサポートする。

【UTMの仕組み】



近年は標的型攻撃に見られるように、特定の企業の機密情報や顧客情報を盗み取り、第三者に転売する金銭目的の攻撃は後を絶たない。「うちは標的型攻撃の被害に遭うような情報は持っていない」と考える経営者もいるかもしれない。だが、対策の手薄な企業がその踏み台になり、取引先が狙われる危険性もある。「標的型攻撃とは無関係」とは言っていられない

。攻撃者の手口が巧妙化し、いくつかのステップを踏んで攻撃を仕掛け、目的の機密情報を盗み取る手口が知られている。その手口を理解し、対策を講じることが、不正アクセスや情報漏えいを防ぐ手立てとなる。

入り口から出口まで複数の対策を組み合わせる

複数のセキュリティ対策を組み合わせた多層防御では、攻撃の入り口となるウイルス感染から機密情報が盗み出される出口まで、ステップに応じた対策を行う。攻撃者が最終目的である機密情報を盗み出すまで、どこかの段階で攻撃に気付き、食い止められれば情報漏えいは起こらない。

攻撃側の手口を大まかに説明すると、5段階になる。それぞれに応じて多層的にセキュリティ対策を組み合わせる。

(攻撃の入り口)システムへの侵入口を探す。

(1)【攻撃の準備】標的とする企業・団体に関係のあるグループ会社や取引先からメールアドレスなどの情報を盗み取る。

(2)【初期潜入】盗み取ったメールアドレスなどを悪用し、関係者になりすましてウイルスを埋め込んだ添付ファイルをメールで送りつけて感染させたり、悪意のあるWebサイトに誘導して未知のウイルスに感染させたりする。

(3)【基盤構築】社内ネットワークに侵入したウイルスが攻撃用の「裏口」をつくり、攻撃者がシステムを操る通信経路を構築する。

(4)【内部調査】社内システムのどこに機密情報が保管されているのか調べたり、そこにアクセスするためのID・パスワードを盗み取ったりする。

(5)【目的遂行】攻撃者は盗んだID・パスワードを悪用してシステムを遠隔操作し、目的の機密情報を選び出す。乗っ取ったパソコンを踏み台にして、他社を攻撃するケースも多い。

(攻撃の出口)機密情報を盗み取る。

ウイルス対策ソフトやファイアウオールだけでは多層防御にならない

セキュリティ対策として、一般的によく知られるものに、悪意のあるメールやWebサイトからのウイルス感染を防ぐウイルス対策ソフトなどのアンチウイルスがある。インターネットからの不正アクセスを監視・防御するファイアウオールと、単機能のウイルス対策ソフトを組み合わせて導入しているケースも多いだろう。だが、これは入り口対策の一環にすぎず多層防御ではない。

入り口対策では、既知・未知のウイルスを検知して感染を防いだり、悪意のあるWebサイトへのアクセスを制限したりする対策が必要になる。個人情報やクレジットカード番号などを盗む詐欺行為をブロックする「アンチフィッシング」、無差別に送られてくる迷惑メールを検知・隔離する「アンチスパム」、従業員が業務に関係のないWebサイトへアクセスするのを制限する「URLフィルタリング」が欠かせない。

出口対策では、攻撃者が遠隔操作するシステムの不審な動きを検知して通信を遮断し、情報漏えいを未然に防ぐといった対策が有効だ。パソコンのデータをユーザーに気付かず送信するのを防ぐ「アンチスパイウェア」、情報漏えいリスクのあるファイル交換サービスの通信を制限する「転送アプリケーション制御」、社内ネットワークの異常な通信を検知・遮断する侵入検知・防御が求められる。

これらのセキュリティ対策を個別に導入することも可能だが現実的とは言い難い。最新の脅威に対応するには、対策に必要な定義ファイルやバージョンをそれぞれ更新する必要がある上に、単体で購入すればその分コストもかかるからだ。

UTMは導入後の運用・サポートで選ぶ

こうした課題に対し、多層防御を実現するのがUTM(統合脅威管理)だ。UTMは複数のセキュリティ機能を1台に統合し、さまざまな脅威に対応する。UTMはセキュリティ対策としてかなり一般的ともいえ、「UTMならもう導入済み」という企業もあるだろう。だがUTMのタイプによってはファイアウオールやウイルス対策など、入り口対策に対応する機能はあっても出口対策

に対応していないものもある。

また、機器だけを導入してその後何もしていない場合は注意が必要だ。UTMのサポートが終了している場合、定義ファイルの更新がされず、新たな脅威にさらされるリスクがある。そんな状態で複数のセキュリティ機能を稼働させると、機器の処理性能が最新のものに比べて見劣りし、業務の効率性に影響を与える。

UTMは国内外の事業者からさまざまなタイプが提供されているので、事業所の規模や必要な機能に応じて製品を選択すればよい。ただしアラートが出ても、システム担当がすぐに対応できなければ、結局攻撃を防げない。サポートがしっかりしている製品のほうが、いざというときに頼りになる。

UTMを導入したものの、定義ファイルの更新など運用管理は面倒なものだ。専任のシステム担当者やセキュリティ担当者を配置しにくい企業はなおさらだ。セキュリティおまかせプラン プライムでは、Biz Box UTM(Cloud Edge 100/50/10)の提供だけでなくUTMのサポートもセットとなる。UTMの稼働状況を24時間・365日専門のセンターで監視し(※)、トラブル発生時には企業へ通知する。UTMの設定変更、最新の定義ファイル更新、ウイルスの検知結果などをまとめた月次レポートの提供も行う。システム担当の専任者がいない企業でも、自社のセキュリティ対策の状況を簡単に把握できる。
※設備の保守・メンテナンスなどによりサービスを停止する場合を除く

UTMは、導入すれば終わりではない。導入後の運用、サポートを考慮して、自社に適した製品・サービスを検討したい。

●この記事のポイント
1.セキュリティ対策は単体では防御になりにくい
2.UTM(統合脅威管理)で多層防御を実現
3.稼働状況監視や更新など、UTMにはサポートが必要
4.中小規模の事業所にはセキュリティをまるごと任せられるソリューションが最適

※掲載している情報は、記事執筆時点のものです