ITで働き方を変える（第13回）

サイバー攻撃の被害を最小化する「初動対応」と「調査・分析」

2024.01.22

サイバー攻撃が巧妙化、高度化する中で中小企業が攻撃の対象として狙われるケースが増えてきている。確固としたセキュリティ対策を講じている大企業をいきなり狙うより、サプライチェーンの構成員である中小企業を攻撃し、そこを踏み台に攻撃対象を拡大する方が効率が良いからだ。規模が小さく、専任のIT管理者もいない中小企業はこの状況にどう対応すれば良いのだろうか。

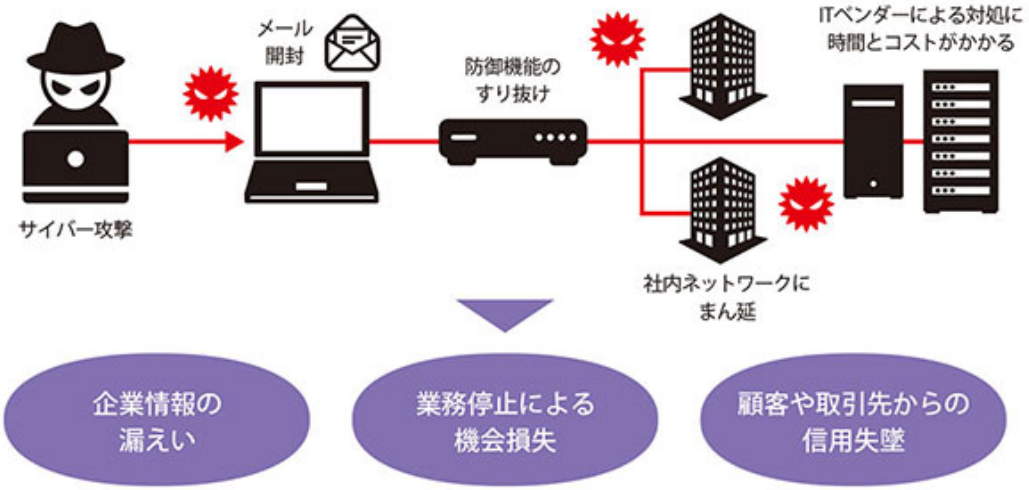
どの中小企業にも求められるセキュリティ対策の強化

昨年から急増しているサイバー攻撃として注目されているランサムウエア攻撃は、不正なプログラムを使って企業が持つデータを暗号化し、使えなくしたところで身代金を要求する攻撃手法だ。サプライチェーンを狙った攻撃の多くがこの攻撃である。

このサプライチェーンへの攻撃で狙われるのが中小企業だ。大企業に比べてセキュリティが脆弱で攻撃しやすく、それを踏み台としてランサムウエア攻撃を広げるケースが増えている。日本でも製造業や医療サービス業などでサプライチェーンを構成する中小企業がサイバー攻撃を受けて被害が拡大したケースが発生した。中小企業も例外ではなく、セキュリティの対策と体制の強化が求められている。

一方、日々進化するサイバー攻撃は高度なセキュリティ機能を導入していても100％防御することはできない。そこで求められるのは、いくつものセキュリティ対策を組み合わせた多層防御である。いかにインシデントの発生を早期検知するのかが問われ、被害拡大を抑止する封じ込めや早期復旧、関連する取引先などへの迅速な報告なども求められる。

●ランサムウエアの感染例



しかし、規模が小さく専任のIT管理者もいない中小企業にとってはこうした仕組みや体制を整えるのは難しい。そこでNTT西日本ではこれまでの多層防御のセキュリティ機能にEDRセキュリティ機能とチャット連携機能を加えてパワーアップした「セキュリティおまかせプラン プライム plus」の提供を開始した。

NTT西日本に任せて安心のセキュリティ対策サービス

「セキュリティおまかせプライムプラン」ではこれまでのインターネットの出入り口の通信の保護監視と標的型メール訓練機能、パソコンのセキュリティ保護機能に加えて、新たにエンドポイントでの不正の検知と対応を行うEDR(Endpoint Detection and Response)セキュリティ機能と、チャットの「elgana」と連携した通知機能が追加された。

EDRとは、端末などエンドポイントの操作や動作の監視を常時記録し、そこから不正な挙動の兆候をいち早く検知して、必要に応じて端末をネットワークから隔離し、攻撃の中身を調査・分析をすることで被害を最小化することを主な目的とする。だが、相応のスキルがなければ運用自体が難しいという側面もある。

そこで「セキュリティおまかせプラン プライム plus」ではインシデント発生時の初動対応支援などを行うマネージドEDRなどが提供されている。また、セキュリティの専門企業であるトレンドマイクロの専門部隊が24時間365日監視し、インシデントが発生した際にはユーザー企業に代わって必要な処置をとり、最終的な報告まで対応してくれる。

さらに、チャットサービスである「elgana」と連携することで、緊急度の高いアラート通知がリアルタイムに確認できることで、迅速に次のアクションにつなげることが可能になる。

UTMとEDR機能がセットになり、手厚いサポートが提供される「セキュリティおまかせプラン プライム plus」であれば、専任のIT担当者の不足などに悩む企業の支えとなるだろう。セキュリティ強化といってもどこから手をつけて良いかわからない場合でも心強い存在だ。

本サービスの担当者によると、従来のプランの契約数はすでに3万件を超え、コロナ禍でテレワークにシフトした顧客の機密情報を扱う広告業や外国労働者のビザやパスポートの情報を扱う人材派遣業など、任せて安心というメリットを享受している中小企業は多いという。働き方の多様化によるエンドポイントの拡大などを背景に、今は規模が小さいからサイバー攻撃を受けないということはなく、UTMが導入されていれば大丈夫ということはない。どんな企業にもしっかりしたセキュリティ対策と対応が求められる時代にあって、責任を果たしながら安心してビジネスに専念するために最適なサービスと言えるのではないだろうか。

※掲載している情報は、記事執筆時点のものです