事例で学ぶセキュリティインシデント（第2回）

取引先に送ったメールの添付ファイルがウイルス感染

2023.07.21

「御社から送られてきたメールの添付ファイルがウイルスに感染しているようです。調べてもらえますか」

西日本で日用品を販売する小売業のB社。取引先からの電話でウイルス感染のインシデントが発覚した。報告を受けた本社の情報システム担当者は、「メールを受け取った相手先からの指摘でウイルス感染が発覚することがある」との事例を聞いてはいたものの、「まさか、うちが……」という思いだった。

そして、ウイルス感染のメールを送信した相手はその取引先だけなのか、他にも送信している可能性はあるのか、自社・店舗でウイルス感染の被害はあるのかなど、早急に調べなければならないことが山ほどあるのを悟った。

メールやWebなど複雑化するウイルス感染経路

コンピューターウイルスの脅威は古くて新しい問題だ。パソコンやサーバー、スマートフォン、タブレットなどのデバイスに侵入し、プログラムの破壊やファイル削除、機密情報の窃取などを行う不正なプログラムだ。プログラムに寄生して感染を広げるタイプの他、ネットワークを介して増殖するものや、正規のプログラムを装い、ユーザーが実行すると悪意のある振る舞いをするものなどもある。

こうした悪意のあるプログラムを総称して「マルウエア」と呼び、ウイルスはマルウエアの一種と言える。また、パソコンやサーバーに感染させてデータをロックし、解除のために身代金を要求する「ランサムウエア」もマルウエアに含まれる。

ウイルス感染の手口も昔と今では変わっている。かつては攻撃者の自己顕示欲からウイルスを作成、不特定多数に感染させる愉快犯的な手口が多かった。近年は特定の企業・組織の機密情報や金銭の窃取を目的にメールやSNS、Webを悪用してウイルス感染させるといったように手口、経路も複雑化している。

感染メールを受け取ったとしても、基本的にそれだけでは感染はしない。ウイルスが含まれる添付ファイルを開いたり、メールやSNSに記載された悪意のあるWebサイトのリンクをクリックしたりすることでウイルスに感染するケースが多い。感染するとデバイスが異常な動作をしたり、保存された情報が盗まれたりする恐れがある。

表計算ソフトのマクロ機能を悪用してウイルス感染

B社は西日本に5店舗を構え、日用品・生活雑貨の小売業を展開する。従業員は店舗のパート・アルバイトを含め70名ほどだ。専任の情報システム部門はないものの、本社の管理部門がIT活用に関する業務を担っている。本社・店舗では特に機密情報を扱うわけではないが、POSシステムやパソコン、ファイルサーバーなど、多様なIT環境の拡充とともにセキュリティ対策にも留意してきた。パソコンは本社と店舗、取引先とのメール連絡の他、ホームページの閲覧・更新などにも利用される。

情報システム担当者は、ウイルス感染を指摘してくれた取引先に連絡を取り、インシデントの経緯を調査。B社の仕入担当

者から送信されたメールが取引先のウイルス対策ソフトに検知され、ウイルス感染の可能性がある旨の警告が表示されたという。

仕入担当者に事情を聞いたところ、本人は添付ファイルがウイルスに感染していたとは知らずに取引先に表計算ソフトで作成した注文書をメールに添付して送信。ただ、正規の手順とは異なる方法でメールを送信していた。本来は出社してからメールを送信する決まりだったが、担当者は午前中に外出する予定があったため、自宅のインターネット回線からメールを送信したという。

B社では、社内ネットワークと社外のインターネットの境界(ゲートウェイ)でウイルス対策やファイアウォールなどのセキュリティ対策を実施している。社内ネットワーク上であれば、ウイルス感染を検知できた可能性があるが、自宅から直接、取引先へ送信したため検知できなかった。端末レベルのウイルス対策(エンドポイントセキュリティ対策)をしておらず、結果として仕入担当者は意図せずにウイルス感染したメールを送ることになってしまったのだ。

そして、B社のIT環境をサポートしている事業者に仕入担当者のパソコンを調べてもらい、いわゆる「マクロウイルス」であることが判明した。これは表計算ソフトなどオフィスソフトのマクロ機能を悪用して自己増殖するウイルスだ。

パソコンなどのエンドポイントセキュリティを強化

情報システム担当者は、取引先にウイルス感染メールを送付した経緯を迅速に説明し、謝罪した。そして、他の取引先や社内にウイルス感染被害が広がっていないか調査した。仕入担当者は指摘のあった取引先にしかメールを送っておらず、他の取引先には被害が及んでいなかった。また、仕入担当者はその日、社外で仕事をしていたため、ウイルス感染したパソコンを社内ネットワークに接続しておらず、取引先からの指摘も早かったので社内へのウイルス感染は免れた。

だが、情報システム担当者はウイルス対策ソフトの定義ファイルを最新版に更新し、念のために社内のパソコンとサーバーが感染していないかどうかチェックを重ねた。ウイルス感染したパソコンは事業者のサポートを受けてウイルスを駆除した後、社内ネットワークに接続した。

その後、全従業員にウイルス感染インシデントの経緯を説明し、ルールに従ってセキュリティ対策が施された社内ネットワークからメール送信することや、不用意に添付ファイルを開かない、メールに記載されたURLにアクセスしないことなどを徹底するように通達した。そして、情報システム担当者は管理部長とともに経営層にインシデントの経緯を説明し、セキュリティ対策の強化を提言した。具体的には、仕入担当者のように社外でパソコンを利用するニーズに対応するため、ゲートウェイでのウイルス対策に加え、エンドポイントでのウイルス対策を行う。これにより、セキュアな環境で柔軟な働き方にも対応できるというものだ。

また、取引先との受発注はメールに変更し、社内・社外にかかわらず、インターネット接続環境があればどこからでも利用できるクラウドストレージの導入を検討することになった。仕入担当者の発注情報だけでなく、さまざまな情報をクラウドストレージ上で一元管理することで、本社・店舗・取引先との情報共有も安心・容易に行えるようになると見ている。このように、B社では今後を見据え、ウイルス感染のインシデントを1つのきっかけとして社内のIT環境とセキュリティ対策を再点検し、改善している。