事例で学ぶセキュリティインシデント（第19回）

セキュリティパッチ適用を怠りインシデント発生

2024.12.16

関西で日用品の卸売業を展開するS社では本社と営業拠点をインターネットVPNで接続し、販売データや新製品などの情報を本社のファイルサーバーに保管、共有してきた。そのファイルサーバーがマルウエアに感染し、情報を閲覧できなくなるインシデントが発生。本社の総務兼IT担当者はVPN機器のぜい弱性を突いたサイバー攻撃を疑った。営業拠点のVPN機器を含め、セキュリティパッチの更新を怠っていたからだ。今となっては、ランサムウエア感染ではないことを祈るばかりだった。

ソフトの不具合を修正するプログラム

パッチとは、いわば「つぎあて」のこと。手芸で小さな布切れを縫い合わせるパッチワークがおなじみだ。転じてIT分野のセキュリティパッチとは、WindowsなどのOS（基本ソフトウエア）や各種ソフトウエアのぜい弱性や不具合を解消するための修正プログラムを意味する。

ソフトウエアの開発時点で見つからなかったバグなどの修正プログラムを開発元がユーザーに提供する。多くの企業が業務で利用しているWindowsの場合、定期的にアップデートを行い、セキュリティパッチの提供や機能の改善を続けていることもその一例だ。

攻撃者がパソコンやサーバーのセキュリティホール（セキュリティ上の穴、ぜい弱性）を狙ってウイルス感染やシステムの不正侵入、プログラムの書き換えなどの被害を与える攻撃手法は以前から知られている。ウイルス対策ソフトなどを開発するセキュリティベンダーがセキュリティホールの穴をふさぐセキュリティパッチを提供。ユーザーはインターネットを介してパソコンに修正プログラムをダウンロードしたり、社内のサーバーから各パソコンに配布したりするなどセキュリティパッチを適用し、セキュリティ対策を講じる必要がある。

パッチ公開に合わせたゼロデイ攻撃も… 続きを読む