中小企業も標的に

サイバー攻撃

「サイバーセキュリティお助け隊」報告書公表

独立行政法人情報処理推進（IPA）は6月15日、「中小企業向けサイバーセキュリティ事後対応支援実証事業（サイバーセキュリティお助け隊）」の成果報告書を公表した。

本事業は、19府県8地域（①岩手、宮城、福島、②新潟、③長野、群馬、栃木、茨城、埼玉、④神奈川、⑤富山、石川、福井、⑥愛知、⑦大阪、京都、兵庫、⑧広島、山口）の中小企業を対象に、サイバー攻撃被害の実態などを把握するとともに、サイバーインシデントが発生した際の支援体制の構築に向けた実証事業である。1064社の中小企業が参加し、そのうち727社に対してUTM（統合脅威管理）などのセキュリティー機器を設置し、サイバー攻撃の実態把握を行った。

本実証を通じ、中小企業においても規模や業種を問わず例外なくサイバー攻撃を受けている状況が確認されるとともに、検知および防御のための対策や社内体制の構築ができていない企業が多いことが確認された。また、全国8地域合計で128件の電話およびリモートによるインシデント対応を行い、そのうち18件の駆け付け対応を行った。駆け付け対応を行った事例を紹介する。

駆け付け対応事例

■事例①

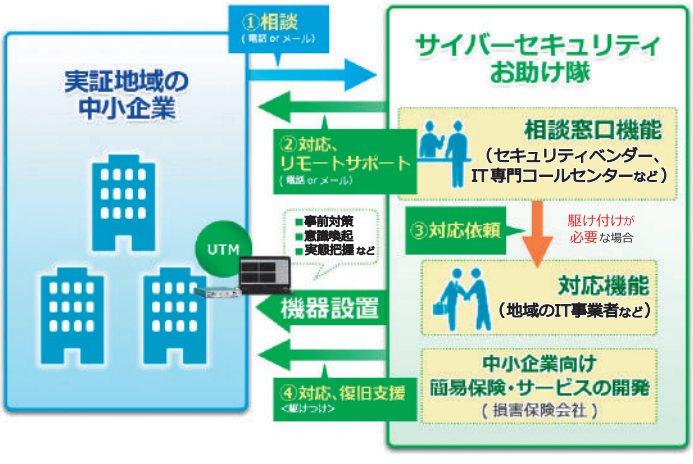
過去に複数のウイルスの通信先として使われたIPアドレス宛ての通信をUTMが検知した。当該企業に確認したところ、ウイルス対策ソフト未導入のWindowsXPパソコンにて通信をしたことが判明し、ウイルス駆除のため駆け付け対応を実施した。

ウイルス感染端末は、WindowsXPでしか動作しないソフトウエアを利用するためのもので、インターネットに常時接続していない認識であったことから、ウイルス対策ソフトが導入されていなかった。今回、プリンターを使用するために社内LANに接続したことで、意図せずインターネットに接続されていたことが判明した。当該端末に対しウイルススキャンを実施したところ、ワームやトロイの木馬、迷惑ソフトなど計25ファイルの不正プログラムを発見したため駆除を実施した。

■事例②

UTMが2カ月間で100件のウイルス付きメールを検知・ブロックしている状況を確認した。検知数が多いため追加調査が必要と判断し、駆け付け対応を実施した。

取引先企業のメールサーバーが不正アクセスを受けたことで当該企業のメールアドレスが漏えいし、それが悪用されて「賞与支払い」「請求書支払い」などを装うなりすましメールで標的型攻撃を受けていたことが判明した。当該企業に標的型攻撃の対象になっていることを通知し、ウイルス付きメールはUTMでブロックしている状況ではあるが、被害が拡大しないよう従業員へ注意喚起した。



「サイバーセキュリティお助け隊」のイメージ

成果報告書ではこれ以外のインシデント駆け付け対応事例のほか、組織的なセキュリティー対策の実態や人的リソースの状況などのアンケート結果が掲載されている。自社のセキュリティー対策実施の参考にしてほしい。また、本事業は今年度も地域を選定して実施予定である。対象地域の事業者は対策強化に向けてぜひ活用してほしい。

（独立行政法人情報処理推進機構・江島将和）