事例で学ぶセキュリティインシデント（第3回）

取引停止の恐れもあるサプライチェーン攻撃

2023.08.18

「パソコンの動作がちょっとおかしいようです。もしかしたら、ハッキングされたのかもしれません……」

始業開始とともに、設計部の社員から管理部に緊急の電話がかかってきた。電話を受けたIT担当者は、パソコンの電源を切り、ネットワークから切り離すように指示して受話器を置いた。「近年、サプライチェーン攻撃が増えているので注意するように」との連絡を取引先から受けたばかりだ。万一、ハッキングされたとしたら大変なことになる。社内・社外に影響が及んでいなければいいが――と願いながら、IT担当者は設計部の部屋に向かった。

対策が手薄な中小企業が狙われる

自社の得意分野を生かした製品・サービスを提供し、多種多様な関連企業が集まってモノづくりのプロセスを遂行するサプライチェーン。そのサプライチェーンを狙ったサイバー攻撃が増えている。

「うちは中小企業だから攻撃者に狙われるような機密情報はない」と高をくくる経営者もいるかもしれない。だが、サプライチェーン攻撃で狙われるのは、中小企業が多いのも事実。サプライチェーンを構成する大手企業はセキュリティ対策に力を入れており、攻撃者にとってハードルが高い。一方、中小規模の取引先や業務委託先はセキュリティ対策が手薄なケースもあり、攻撃を仕掛けやすいとされる。

そして、攻撃された中小企業のパソコンやサーバーを踏み台に取引先の大手企業のシステムに侵入して機密情報を盗み取ったり、ウイルスに感染させたりする手口がある。攻撃を仕掛けられた中小企業は、結果的に取引先に損害を与えることになり、取引停止によるビジネス機会の逸失や売り上げ減少による経済的な損失を被る。社会的な信用を失い、事業の継続や雇用の確保などにも大きな影響を与える恐れがある。

サプライチェーン攻撃が深刻になる一方、大手企業は取引先にも自社と同様のセキュリティレベルを求める傾向にある。新製品の設計データなどを取引先と共有しながらモノづくりを進めるサプライチェーンでは、データ保護はもちろん、独自のノウハウや知的財産などを含めた機密情報保護が重要になる。そのため、取引先、業務委託先に対して、サイバーセキュリティ対策のレベルを確認した上で契約を交わす例もある。

パスワードの使い回しで不正アクセス… 続きを読む