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

C社は関西に拠点を構え、自動車部品メーカーで構成されるサプライチェーンの一角を担う。従業員は100名ほどの企業だが、品質の高い部品を供給し、取引先とも良好な関係を築いてきた。専任の情報システム部門はなく、管理部の社員がIT担当を兼務する。サプライチェーンの中核を担う大手部品メーカーからは定期的にセキュリティ対策の報告を求められ、IT担当者が対応してきた経緯がある。

IT担当者は設計部から管理部へ不正アクセスの疑いのあるパソコンを持ち帰るとともに、連絡してきた社員から事情を聞い

た。朝、出勤してパソコンを立ち上げたところ、いつもより動作が遅いことに気付いたという。そして、パソコンの中に見覚えのないファイルがあったことからハッキングを疑い、管理部に電話したという。

設計部のパソコンは自動車部品メーカーから提供されるCADデータを扱うため、他のパソコンよりもスペックが高く、ウイルス対策などセキュリティにも留意してきた。まず、攻撃の手口として考えられるのがソフトウエアのぜい弱性を悪用した不正アクセス。ソフトウエアにウイルスを仕掛け、バージョンアップ時などに感染させる。設計部のパソコンは定期的にソフトウエアのバージョンアップを実施しているが、当該パソコン以外は攻撃の痕跡もないことから、他の手口が考えられる。次に考えられるのがIDやパスワードの不正利用だ。ID、パスワードはパソコンのログインの他にも、ファイル共有などのアプリケーション利用時にも入力が求められる。管理部では従業員に対して定期的なパスワードの変更を求めてきたが、いくつものパスワードを覚えきれないといった理由から、同じパスワードを使い続けている人もいるようだ。

パソコンが不正アクセスされた設計部の社員もそうした1人だ。プライベートで使用しているパスワードと同じものを業務でも使い回していたという。攻撃者は解析ソフトを悪用してパスワードを調べ、盗み取る。いくら不正アクセスの対策を講じていても、攻撃者が本人になりすまし、盗み取った正規のID、パスワードを使ってログインするため不正アクセスを防ぎにくいという問題がある。

多要素認証でパスワードを強化

C社ではITの構築・運用をサポートしてもらっている事業者に連絡を取り、設計担当者が見覚えのないというファイルを削除するとともに、ウイルス対策ソフトの定義ファイルを最新版に更新してスキャンした。パソコンのログを調べたところ、サーバーなどを不正操作した形跡が見当たらなかったため、当該パソコン以外は被害がなかったと判断した。ただ、念のため、サプライチェーンの大手部品メーカーには不正アクセスのインシデントが発生したことを報告した。

そして、C社の全社員に対してパスワードの使い回しは止め、推測が難しいパスワードに改めるよう周知・徹底を指示。さらにパスワード管理の強化策として、多要素認証の導入を決めた。多要素認証は、ID、パスワードに加え、本人固有の生体認証や、ログインするたびにパスワード（認証コード）が変わるワンタイムパスワードなどを組み合わせることで不正アクセスを防御する効果がある。

また、攻撃者の遠隔操作など不正な通信を検知・ブロックする機能を備えるUTMの導入や、パソコンのセキュリティを強化するエンドポイントセキュリティの導入も今後の検討事項となった。サプライチェーン攻撃を防ぐには、取引先との情報管理規則を徹底することや、信頼できる取引先を選定すること、取引先と情報セキュリティの責任範囲を明確にして合意を得ることなどがポイントとなる。

C社では今回のインシデント発生を教訓に、サプライチェーンを構成する1社として信頼され、継続的に選ばれる企業となるためにセキュリティ対策を強化していく考えだ。