事例で学ぶセキュリティインシデント（第7回）

対策が手薄になりがちなリモート拠点が狙われる

2023.12.14

情報システム担当者などの管理者を配置しやすい本社などの主要拠点に比べ、セキュリティ対策が手薄になりがちなのが小規模な支店・営業所などのリモート拠点だ。社内だけでなく、社外の顧客・取引先を含めさまざまな相手先と情報をやり取りしながらビジネスを進める今日、リモート拠点のセキュリティ対策が重要になる。攻撃者はリモート拠点を踏み台に本社や取引先への不正侵入を試みるなどのリスクもあるからだ。今回は、そんなリモート拠点のインシデントの事例を紹介する。

VPN機器の認証情報を悪用して不正アクセス

昨夜、支店のネットワークが不正アクセスされ、パソコンに保存されたデータが盗まれたかもしれません。どうすればいいでしょうかーー。G社の管理部門と情報システム部門を兼務する担当者に支店長からあわてた声で電話がかかってきた。事情を聞くと、出勤してパソコンを立ち上げるとウイルス対策ソフトからコンピューターウイルス侵入の警告が表示され、驚いて本社に電話をかけたという。まず、そのパソコンを支店のネットワークから切り離すように指示し、パソコンを調べるため本社に届けるように伝えた。「もしかしたら、本社も不正アクセスされているかもしない。早急に手を打たなければ」。

G社は大阪の本社の他、西日本に3つの支店を構え、従業員数30名ほどの建設会社だ。時間外労働の制限など2024年問題の解消に向けて働き方改革に取り組み、その一環として建設現場や支店でのIT活用に力を入れる。例えば、建設現場で働く従業員にタブレット端末を支給し、紙の図面に代えてタブレット端末に図面を表示したり、日々の業務報告も現場で行えるようにしたりするなど業務の効率化を進めてきた。

本社と各支店はVPN（仮想閉域網）で接続し、設計図面や建築資材、労務管理、業務報告などのさまざまな情報をやり取りしている。VPNはデータの暗号化や認証技術を用いて情報を安全にやり取り可能な通信手段として多くの企業が導入し、本社とリモート拠点の接続やテレワークなどで利用されている。通信事業者などが提供するVPNサービス（IP-VPN）と、自営のVPN機器とインターネットを用いて通信するインターネットVPNに大別できる。

そのVPN機器を狙ったサイバー攻撃がある。VPN機器の認証情報(ID、パスワード)を盗み取ったり、VPN機器のぜい弱性を突いて攻撃を仕掛けたりするなどの手口だ。対策としては、VPN機器にアクセスする際のパスワードの使い回しを止める、異動や退職などで使われなくなったID、パスワードを削除するといった認証情報の管理を徹底する必要がある。

VPN機器のぜい弱性については、必ずしもすべての機器がぜい弱性の対象となるわけではなく、メーカーの機器やOSなどのバージョンによって異なる。ぜい弱性に関する情報は機器を提供するベンダーやセキュリティ関連組織がホームページなどで公表しており、もし、対象となる機器・バージョンを利用している場合、ベンダーが公開する修正プログラムを直ちに適用するといった対策が必要だ。

パスワードの使い回しなどの実態が明らかに

G社では本社と各支店にVPN機器を設置し、自営のインターネットVPNを構築・運用してきた。攻撃者が何らかの方法で盗

み取った従業員のID、パスワードを悪用してVPN機器に不正アクセスし、支店のネットワークに接続されたパソコンがウイルス感染した恐れがある。

支店長が本社に持参したパソコンをセキュリティ専門会社に調べてもらったところ、ウイルス侵入の痕跡はあったものの、パソコンに保存された情報の流出は確認されなかった。また、支店のVPN機器を介した本社ネットワークへの不正アクセスについても確認されず、幸いにも情報流出はなかったと判断した。そして、専門会社の手を借りて該当パソコンのウイルスを駆除し、復旧させた。

ただ、情報システム担当者は、ネットワークが不正アクセスされ、サーバーやパソコンがランサムウエアなどに感染すれば大事になると懸念していた。そして、不正アクセスの要因となった、支店のVPN機器に接続する従業員のID、パスワードが第三者に盗まれた可能性があることを問題視した。

支店従業員に日頃のパスワード管理について尋ねたところ、多くの課題が浮かび上がった。例えば建設現場に持ち込むタブレット端末やノートパソコンのパスワード入力を周囲の目を気にすることなく行っていたり、システム利用時と同じものを使い回していたりする実態が明らかになった。建設現場では自社以外の人も出入りしている。また、現場近くのカフェなどで休憩中に端末を立ち上げて工事の進捗（しんちょく）などを確認することもあるという。そうした場所で悪意のある第三者にID、パスワードが盗み見され、不正アクセスに利用された可能性もある。情報システム担当者は支店の不正アクセスの経緯を経営層に報告するとともに、全社員に対して定期的なパスワード変更や、推測されやすいパスワードは避けることなど管理の徹底を通達した。

脅威の多様化とともに進化するUTMの導入を検討

今回のインシデントはVPN機器への不正アクセスに端を発したものだが、管理の目が届きにくいリモート拠点が攻撃者に狙われた。そこで、本社・各支店のVPN機器をはじめ、ネットワーク機器、サーバー、パソコンなどに対して最新のセキュリティパッチを適用するとともに、インターネットVPNから通信事業者が提供するIP-VPNサービスへの変更を検討することになった。事業者のサービスを利用することにより、リモート拠点の通信環境を一元管理しやすくなると見ている。

G社では、インターネットと社内ネットワークの出入り口となる本社のゲートウエイにファイアウォールを設置していたが、インシデントを受けて新たにUTM（統合脅威管理）の導入を検討。セキュリティの脅威が多様化するとともに、UTMの機能も進化しており、標的型サイバー攻撃やランサムウエアの侵入検知、遠隔操作などの不審な通信を検知・防御する機能を備えたUTMや遠隔監視などのサービスを組み合わせたソリューションも候補になるからだ。また、従業員のセキュリティ意識の向上にも重きを置いた。パスワード管理の徹底はもちろん、万一、不正アクセスやウイルス感染などの攻撃に遭ったと思われる場合、自分だけで判断せずに速やかに管理職や情報システム担当者に報告するなど対応の手順を決めた。建設業は人手不足が深刻な上、長時間労働などの見直しが求められている。G社ではITを活用した働き方改革をさらに推進するためにも、リモート拠点を含めセキュリティ対策に力を入れていく考えだ。