サイバーセキュリティ最前線

急増する「サプライチェーン攻撃」もはや誰にとっても他人事ではない!!

2024年春、公文教育研究会、クボタ関連会社、複数の地方自治体などが、相ついで情報漏洩あるいはその可能性を公表した。一見すると業種も特徴も異なるが、請求書や通知ハガキなどの帳票類を委託していた印刷業者㈱イセトー)が管理していた個人情報が流出し、委託元である企業・団体が情報管理責任を問われ、公表にいたったのだ。このようにサプライチェーンの一部を踏み台にして、つぎの標的を狙う攻撃のことを「サプライチェーン攻撃」という。

サプライチェーン攻撃の実態

「サプライチェーン攻撃」という概念が登場したのは2010年代前半とされている。当初は特定の企業を狙う際に、その企業が依存するシステムベンダーや協力会社を踏み台にする標的型攻撃とされていたが、現在ではむしろ脆弱性がある企業を無差別に狙い、結果的にその企業の取引先・顧客などに波及するケースが増えている。

その背景にはAIをはじめとしたテクノロジーの進化やサイバー犯罪の一般化がある。実際、セキュリティ専門会社の㈱ブロード(東京都千代田区)は「近年はインターネット上で簡単に手に入るツールやサービスを利用して、高度な知識なしにサイバー攻撃を仕掛けられるようになった」と話す。そして、とくにここ数年は「AIの進化により、攻撃対象の選定や侵入経路の発見が高度に自動化され、セキュリティの弱い企業や組織のネットワークが無差別に被害に遭う傾向にある」とも。

「関係ない」は通用しない

実際、警察庁の2024年調査によると、ランサムウェアによる被害は中小企業に集中しており、被害件数の大半が従業員300人未満の企業に発生。また、業種別で見ると、法令や監督省庁により厳格なセキュリティ基準が求められている金融や医療といった分野では被害が少ない一方、製造業やサービス業、建設業など、比較的、セキュリティ投資が後回しになってきた業種での被害が目立つ。

この傾向は世界的にも共通している。セキュリティインシデント対応を専門とする米国のCoveware社によると、2024年第1四半期に同社が対応したランサムウェア被害のうち、従業員1000人未満の中小企業が全体の約74㌫を占めており、従業員1万人を超える大企業はわずか7・5㌫程度にとどまっている。この点について、前出のブロードは「規模の大小を問わず、インターネットにつながる企業・組織すべてが被害を受ける可能性があり、セキュリティが脆弱な環境を狙って侵害する手口が主流となっている」と警鐘を鳴らす。そもそも、昨今の企業活動は委託・外注・協業など、さまざまなネットワークのなかで行われている。それゆえに「自社は重要情報を扱っていないから」「うちは小規模だから」といった認識では、リスクを過小評価してしまう恐れがあるのだ。

そこで、ブロードでは専任のIT部門を持たない中小企業にこそ導入してほしいソリューションとして、AIによるペネトレーションテスト自動化ツール「RidgeBot(リッジボット)」をあげる。「このツールを導入すれば、専門知識がなくても、攻撃者の視点から自社ネットワークの脆弱性を定期的に検査できる」という。また、エンドポイントのセキュリティ強化策としては「HP Sure Click Enterprise」を推奨。「メール添付ファイルやWeb経由のマルウェアを仮想化された安全な環境で開くことで、PC本体への攻撃を防ぐことができる」というスグレモノだ。そして、いざというときの一手としてはBCP(事業継続計画)対策ソリューション「Neverfail」を提案。このツールがあれば「ランサムウェアなどによってサーバーがダウンした際も、瞬時に稼働環境を切り替え、業務を継続することができる」そうだ。中小企業でも手軽にはじめられる対策として、検討してみるのはどうか。