事例で学ぶセキュリティインシデント（第11回）

感染被害が後を絶たないランサムウエアの脅威

2024.04.22

西日本を中心に事業を展開する建設業のK社。早朝、建設現場事務所の責任者がいつものように本社の工事管理システムにアクセスしようとしたところ、つながらない。「システムが故障したのかな」。始業前ではあるが、本社システム担当者のスマートフォンに連絡した。システム担当者は、急ぎ出社して最悪の事態を悟った。「ランサムウエアにやられた」。上司と役員、電話をくれた現場責任者にインシデントの状況を報告し、まず、何から手を付けるか、深呼吸した。

攻撃者の手口が変化する「ノーウエアランサム」

ランサムウエアの被害が後を絶たない。IPAが毎年公表する「情報セキュリティ10大脅威(組織)」においても、ランサムウエアが1位で脅威の深刻さを物語っている。これは、「ランサム(身代金)」と「ソフトウエア」を組み合わせた造語でウイルスの一種。その言葉通り、パソコンやサーバーに不正アクセスしてデータを暗号化し、データ復元と引き換えに身代金(暗号通貨など)を要求するサイバー攻撃だ。

さらに、身代金を支払わないとデータを公開すると脅迫したり、企業のWebシステムなどに対してDDoS(分散型サービス妨害)攻撃を仕掛けたりすると脅迫する「二重脅迫」の手口もある。攻撃者の手口も変化している。データを盗み取り、暗号化せずに対価(暗号通貨など)を要求したり、支払わないとデータ公開すると脅したりする「ノーウエアランサム」(警察庁の造語)の手口も確認されている。

ランサムウエアに限ったことではないが、攻撃者が企業・団体に不正アクセスする手段としてVPN機器のぜい弱性やリモートデスクトップの認証情報を悪用したり、メールの添付ファイルを悪用したりする手口がある。VPN機器は本社・データセンターと拠点間を閉域網で接続する手段として利用されてきた。テレワークが広がり、VPN機器とインターネットを用いて本社システムと自宅やリモート拠点を閉域網で接続するインターネットVPNを利用する企業も少なくない。すべてのVPN機器にリスクがあるわけではないが、ソフトウエア不具合や設定ミスなどを突いて、攻撃者が不正アクセスを仕掛ける手口が知られている。VPN機器メーカーは不具合を解消するソフトウエアを提供し、企業が適用することで不正アクセスのリスク低減が可能だ。

ランサムウエアの被害は大企業ばかりでなく、中小企業の被害もある。警察庁が令和5年9月に公表した「令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について」によれば、ランサムウエアの被害を受けた企業・団体(103件)のうち、大企業が30件、中小企業が60件、団体が13件となっている。大企業に比べて対策が手薄になりがちな中小企業の被害が顕在化した可能性がある。

VPN機器を経由してランサムウエアに感染… 続きを読む