サイバーセキュリティ最前線

「インシデント損害額調査レポート第2版」からセキュリティ対策の重要性を再確認!!

サイバー攻撃の脅威や対策の必要性がメディアなどで叫ばれるようになって久しい。が、依然として多くの企業・団体が被害に遭った場合の経済的な損失を認識できず、セキュリティ対策の導入に二の足を踏んでいる。そこで、今号ではJNSA（NPO法人 日本ネットワークセキュリティ協会）が公表した「インシデント損害額調査レポート第2版」をもとにサイバー攻撃による被害状況と対策を紹介したい。

拡大するサイバー攻撃被害

2023年9月、JNSA（NPO法人日本ネットワークセキュリティ協会）が、サイバー攻撃の国内被害組織（2017年1月から2022年6月までの間に、被害を公表または報道がなされた1300組織）を対象に「サイバー攻撃によって生じた被害額等に関する実態調査」を実施。2024年にはその調査結果を「インシデント損害額調査レポート第2版」として公表した。調査目的は組織にとって適切なセキュリティレベルを検討してもらうことで、サイバー攻撃被害に遭った組織の規模、業種、サイバー攻撃の種別ごとに集計した統計情報、アンケート調査によって判明した損害額やインタビューによって明らかになった被害の実態を紹介している。

サイバー攻撃の種別は①ランサムウェア（身代金ウイルス）感染②調査時に蔓延したエモテット（一般的なセキュリティ対策では検知しにくいマルウェア）感染③ウェブサイトからの情報漏えい④その他で、被害組織の業種別件数は製造業（280件）、卸売業・小売業（220件）、情報通信業（181件）、サービス業（143件）などと幅広く、被害組織の所在地も全国に広がっていた。また、サイバー攻撃の種別としてはエモテット感染（28ページ）、ランサムウェア感染（13ページ）、ウェブサイトからの情報漏えい（33ページ）といった比率になっており、とくに現在も被害が増加しているランサムウェア感染とエモテット感染が増加傾向にあった。

〝見えにくい損失〟も視野に

では、具体的にどのくらいの損害額が生じているのか。アンケート調査の結果によると、ランサムウェア感染については、被害金額が1000万円超との回答が多く、平均値は2386万円とのことだった。しかし、被害を受けたシステムの停止、データの消失による利益の喪失、機会損失などによる損害額を把握していないケースが多く、実際にはこの数字以上の被害があると想定される。エモテット感染については、被害金額を2000万円以上と回答した組織がある一方で、被害金額が極端に低い組織もあり、平均値は1030万円となっている。また、ウェブサイトからの情報漏えい被害についても組織ごとのギャップが大きく、個人情報のみが漏えいしたケースの平均値は2955万円だったが、漏えいした情報にクレジットカード情報が含まれているケースの平均値は3843万円に達していた。

被害金額の差はあるものの、いずれのケースにおいても中小企業にとっては大打撃になることは間違いない。その点について、セキュリティ専門会社の㈱ブロード（東京都千代田区）は「インシデントが発生すると、通常業務の停滞や担当者の過度な疲弊といった〝見えにくい損失〟が膨れ上がる恐れがある。また、一度損なわれた顧客や取引先との信頼関係を回復するには、長期間にわたる広報・営業活動が必要となり、企業の収益に中長期的な影響を与えることになる」と指摘する。

こうした状況に陥らないようにするには、やはり備えあれば憂いなし、である。そこでブロードでは今、大小さまざまな組織にAIを活用して攻撃者目線でセキュリティ検査を行うことができる「RidgeBot」の導入をすすめているという。自社の弱点や課題の把握にはじまり、個別の課題に応じたソリューションの提案が可能とあって、まさに転ばぬ先の杖となっている。ぜひ導入を検討してみてほしい。