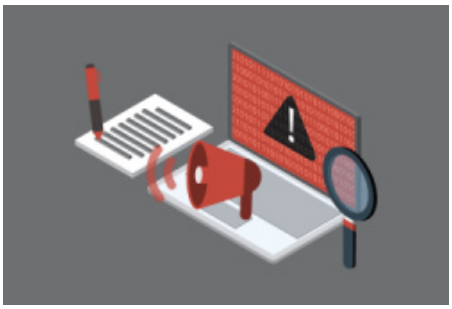
最新セキュリティマネジメント（第24回）

セキュリティインシデント対応は3ステップで

2023.05.29



2023年4月26日に独立行政法人情報処理推進機構（IPA）から「中小企業の情報セキュリティ対策ガイドライン 第3.1版」が発行された。2019年に発行された第3版以来の改訂である。新たに追加されたのが、セキュリティインシデントに関する情報だ。付録には「中小企業のためのセキュリティインシデント対応の手引き」が追加された。この付録を参考にして、今、中小企業に求められるセキュリティインシデントへの対策を考えてみたい。

セキュリティ事故に対して3つのステップで対応する

セキュリティインシデントとは、セキュリティの事故や出来事全般をさす言葉だ。あらゆる企業がサイバー攻撃の対象となっている今、中小企業でもセキュリティインシデントは想定しておくべき事象である。

実際にインシデントが発生した場合には、事業の停止、攻撃者による不正送金、データを人質にとった身代金の要求といった直接的な被害だけでなく、インシデント対応のための人件費、原因調査や復旧のための費用、顧客や取引先への損害賠償などがかかり、間接的には会社の信用力の低下や風評被害なども起こり得る。

こうしたインシデント発生による被害と事業への影響範囲を最小限に抑え、迅速な復旧や再発を防止するために必要となるのがインシデント対応である。目的は、企業としての事業継続性を高めることにある。

付録ではインシデント対応の基本として3つのステップを挙げている。ステップ1は「検知・初動対応」。インシデントが発生している、あるいは発生する兆候をキャッチし、情報セキュリティ責任者が対応の必要性を判断したら、経営者に報告して対応体制を立ち上げる。攻撃を受けた機器を隔離したり、サービスを停止する処置を施したりする。

ステップ2は「報告・公表」。被害の状況をWebサイトやメディアを通じて公表し、顧客や消費者に関係する場合は受付専用の窓口を設ける。被害者や影響を受けた取引先などには対応状況と再発防止策を報告して必要に応じて補償を行い、内容によっては関係する省庁や警察、IPAなどへの届け出も行う。

ステップ3は「復旧・再発防止」。まず5W1Hの観点から状況を調査して、対応方針を決めた上で必要な修復を行ってシステムやサービスを復旧させる。訴訟なども視野にログなどの証拠は保存しておく。さらにインシデントを再発させないために、抜本的な再発防止策を検討して実施する。

このステップ1からステップ3までを普段からしっかり意識しておけば、インシデントによる被害を最小限に抑えられ、事業継続性を高められるだろう。

インシデントごとに異なる、押さえておくべきポイント… 続きを読む