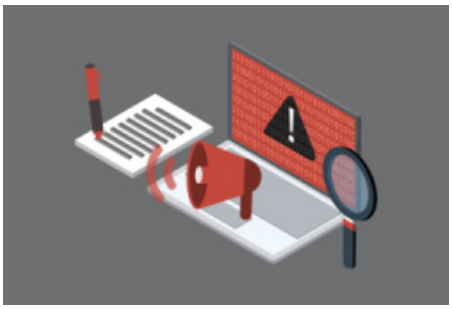
最新セキュリティマネジメント（第24回）

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

ステップ1からステップ3の具体的な内容は、どんなインシデントなのかによっても変わってくる。付録ではウイルス感染とラン

サムウエア感染の場合、情報漏えいの場合、そしてシステム停止の場合に分けて対応策を示している。ここではインシデントごとに押さえておくべきポイントを取り上げる。

ウイルス感染を検知するには、パソコンの動作や通信状況の異常を検知できる仕組みがポイントになる。インシデントが発生した場合には、感染したパソコンやサーバーの利用を停止し、ネットワークから切り離して感染の広がりを防ぐ。再発防止のためには、徹底したウイルスの駆除が重要になる。

ランサムウエア感染では、データのバックアップ体制がポイントになる。感染したパソコンやサーバーをネットワークから切り離し、復号化ツールを入手して復旧を試みる。データをバックアップしているなら、適切な方法で復元(リストア)を行う。これらの方法で復元できなければデータの復旧を断念し、再構築を強いられる場合がある。

情報漏えいの場合には、サーバー対策がポイントだ。不正アクセスを検知してアラートを上げる仕組みや、内部犯行を防ぐために社内システムへのアクセス制御の仕組みが必要になる。インシデントが発生した場合は情報が悪用される恐れがあるので、2次被害を防止するための注意喚起、個人情報保護委員会や警察、IPAなどへの届け出も求められる。

システム停止の場合には、サイバー攻撃かどうか原因が分からないことも想定されるが、優先すべきは事業を止めないことだ。いつでも切り替えられるようにサーバーを冗長化しておく、迅速な対応をとるために事業継続計画(BCP)をあらかじめ策定しておく、などがポイントになる。

IPAのガイドラインなどを活用して、セキュリティインシデントが起きないような対策を講じておくことは大切だ。さらにインシデントが起きてしまったときに適切な対応ができるように準備をしておけば、安心して企業経営に臨める。経営者としても、日頃からそういう視点を持つ必要があるだろう。