最新セキュリティマネジメント（第7回）

リスクに対応するための仕組みの構築

2021.12.21

経済産業省が策定した「セキュリティ経営ガイドライン」で、経営者が社内に対して指示すべきポイントとして示された「重要10項目」。今回は5番目の項目「サイバーセキュリティリスクに対応するための仕組みの構築」について解説する。

リスクに対する組織としての取り組み

経済産業省と独立行政法人情報処理推進機構（IPA）が共同で策定した「サイバーセキュリティ経営ガイドライン Ver2.0」では、企業のIT活用を推進する上で経営者が認識すべきサイバーセキュリティに関する原則や、経営者がリーダーシップをもって取り組むべき項目がまとめられている。

企業が直面するさまざまな形態、手法のサイバーセキュリティリスクに対応するためには、万一のインシデント発生に備え、日ごろから十分対策を講じておく必要がある。リスクに応じた適切な対応が行われない場合、サイバー攻撃の被害は急激に拡大し、結果として業務停止や信用失墜といった深刻なダメージをもたらすことになるのは明らかだ。今回は具体的な対策の内容と、技術・運用両面での取り組みについて解説する。

セキュリティ対策は「防御・検知・分析」

サイバーセキュリティリスクから企業を守るための対策は、大きく「防御・検知・分析」の3種類に分けられる。まず防御の部分では、時を選ばず、さまざまな方法で企業のシステムに襲いかかるサイバー攻撃に備え、被害を最小限に抑えることのできる強靱（きょうじん）な「守り」を固めておく必要がある。

検知の部分では、日常の業務で生じる小さな事象からサイバー攻撃の発生、もしくは今後の攻撃につながる可能性をいち早く察知することがポイントだ。実際に、発見が数時間遅れたため対応が後手に回り、その結果深刻な被害を受けるという例は後を絶たない。夜間や休日を含め、常に監視の目を緩めず対応する仕組みの構築が求められる。そして分析は、検知された事象を詳しく調査して危険性の有無や、予想される被害の規模を確認し、危険と判断した際には直ちに対策実行を指示する役割を担っている。

これまで、企業におけるセキュリティ対策は情報システム部門が中心となり、主に技術面を重視しながら進められてきた。しかし最近は、サイバーセキュリティリスクを企業全体の問題と認識し、経営者をはじめ全従業員が課題意識を持って臨むことが求められている。多額の予算を投じ、最新テクノロジーを駆使した対策を行ったとしても、適切な運用がされなければサイバー攻撃の状況を正確に把握できない。本ガイドラインでは、攻撃者に重要情報を窃取されるといった重大な被害に発展することのないよう、各部署が協力して綿密な対策を講じる必要性を指摘している。

多層防御と監視でリスク対応力をアップ… 続きを読む