情報セキュリティマネジメント試験合格講座 午後試験対策 08

- インシデントマネジメント

1. 脆弱性対応
   脆弱性情報を収集し、自組織のシステムに対する脅威を分析して、必要に応じてパッチ(修正ソフト)の適用や設定変更を行う。

2. インシデントハンドリング
   情報セキュリティインシデントが発生した際に、通報を受け、状況を踏まえ対処方針を決定し、問題解決を行い、インシデントを収束させる。インシデントハンドリング(緊急対応)は、主に以下の4つの機能で構成される。

   (1) モニタリング(事象の検知、報告受付)
   (2) トリアージ(事実確認、対応の判断)
   (3) インシデントレスポンス(分析、対処、エスカレーション、連携)
   (4) リスクコミュニケーション(報告・情報公開)

3. 事象分析
   発生した情報セキュリティインシデントに関するデータを分析し、原因や再発防止のための改善点を明らかにする。

4. 普及啓発
   情報セキュリティインシデントの発生を低減するため、エンドユーザである従業員向けに教育・啓発活動を行う。

5. 注意喚起
   情報セキュリティインシデントにつながるミスや情報セキュリティインシデントの発生時に、関係先に必要な注意喚起を行い、インシデントの被害拡大を防ぐ。

6. その他のインシデント関連業務
   例えば、対処計画が適切に機能するか確認するため、模擬的に情報セキュリティインシデントの発生を設定し、関係者の行動を検証する予行演習などの演習を行うことが考えられる。

7. サイバー攻撃の初動対応

サイバー攻撃を検知した場合、対外接続されているネットワークを遮断したり、攻撃対象となっているサービスを停止したりすることで、外部への情報流出や外部からの不正操作を停止させる効果が期待できるが、これらの操作によって社内の業務や社外とのコミュニケーションが不可能になってしまう弊害もある。ログなどの分析で検知した場合は、検知の時点で、すでに情報が流出してしまっている可能性も高く、遮断や停止を行うことによる効果は必ずしも期待できない。これらを踏まえて、どのような状態に至った場合に、サービスを停止するかといったことも事前に検討しておく必要がある。例えば、以下のような場合には、原因究明や被害拡大を避けるためにサービスを停止することが考えられる。

(1) マルウェア感染の疑いがあり検査をする必要がある場合
(2) 脆弱性があるシステムやサービスを停止し改修や設定変更する場合
(3) 不正に外部との通信を行っている場合
(4) 特定のファイルを変更または削除し続けている場合

サービス停止の検討を行う主体は、経営者や事業部門トップとの合議により判断される場合や、特定の事態において権限を移譲された CISO などが判断する場合など、企業の形態により様々である。

さらに、サービスの復旧についても検討すべき事項は多数ある。サービス妨害攻撃(DDoS 攻撃)の場合、サービスを復旧させた途端に攻撃が再開されることもある。

脆弱性を悪用した攻撃の場合は、脆弱性に対処した後であれば再開しても問題ないと考えられがちだが、すでに社内ネットワークに攻撃用のボットが仕掛けられている可能性もあり、外部接続の再開とともに社外にある C&C サーバ(コマンド&コントロールサーバ:攻撃の指令を行う)との通信が復活することで、攻撃が再開されることもある。

これらを踏まえると、復旧などの判断を行う際には、サイバーセキュリティ関連サービスのベンダやコンサルタントの支援を得るのが適切と言える。しかしながら、初動の直後はこうした外部リソースをすぐに活用できるとは限らないため、ログから検知される内容や状況に応じて対処すべき内容をまとめた手順書などを整備することが望まれる。

8. 事後対応事項
インシデントが落ち着いたところで行うのが、原因究明と再発防止策の策定である。インシデントに至った原因を明らかにした上で、再発することがないようにサイバーセキュリティ対策や業務手順の見直しを図り、PDCA サイクルを通じて全社に反映させる。

9. CISO に求められること
CISO は、サイバーセキュリティ対策を実施する現場と経営層を繋ぐ通訳となることが期待される。

例えば、経営層やステークホルダに対して、自社のサイバーセキュリティリスクの状況や課題を、なるべく技術的な専門用語を使わずに説明し、合意を得る必要がある。またサイバーセキュリティ対策を推進していく上で、事業部門などの現場から手間が掛かるなどの理由で反発を招かないように、現場の立場で支援するというスタンスが求められる。

10. CISO の役割
組織の規模などに応じて、CISO が担う役割は様々であるが、役割の例として下記のようなものが考えられる。

(1) セキュリティポリシを策定する。
(2) サイバーセキュリティリスク管理体制を構築する。
(3) 自社のサイバーセキュリティリスクを把握し、リスク対応計画を策定する。
(4) 対策実施に掛かる費用について経営層の承認を得る。
(5) 構築した体制を維持、改善するための PDCA サイクルを統括、監督する。
(6) インシデント対応の陣頭指揮を執る。
(7) 新規 IT 導入時など、事業部門に対するセキュリティの技術的観点からのアドバイスをする。

なお、あらゆる役割をCISOなどが1人で担うことは難しい場合もあるため、CISO室などの組織を設けて、CISO などを支援するチームを構成し対応するケースもある。また、外部から CISO などやその補佐となる人を招聘したり、CISO などの役割の一部を外部の専門家に委託したりする場合もある。近年 CISO をレンタルするサービスを提供する事業者も現れている。

11. サイバーセキュリティ経営とISMS

情報セキュリティマネジメントシステム(ISMS)には、「サイバーセキュリティ経営ガイドライン」に記載しているサイバーセキュリティリスク管理体制と同などな体制が存在している。例えば、CSIRT を整備していない場合でも情報セキュリティインシデントへの対応や情報セキュリティ事象に関する報告が定められており、サイバー攻撃を受け被害が発生した場合の対応や報告する役割が存在する。

一方、昨今の標的型攻撃は巧妙化、高度化しているため、日々新たなリスクを発見し、速やかに対策することが求められる状況である。サイバーセキュリティの対策は、ISMS で想定している1年や半年の PDCA サイクルでは対応できないため、サイバー攻撃の情報収集や対策の改善などを短いサイクルで実施することが求められる。

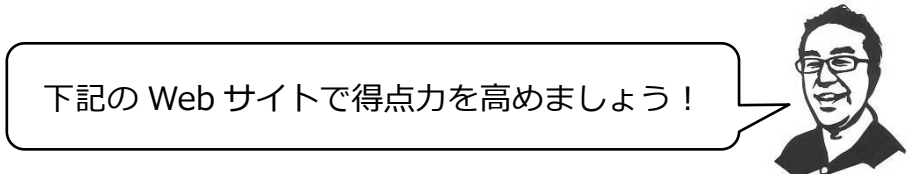
12. 個人情報保護管理体制

個人情報保護法に対応した個人情報保護管理体制が必要である。管理体制は、一般的に個人情報保護管理責任者が存在し、管理委員会や管理を監査する個人情報保護監査責任者も存在する。

一方、管理対象となる情報資産は、個人情報に限定しているため、保護対象の情報資産を企業の重要な情報に拡大して検討する必要がある。例えば、個人情報取扱事業者は、法の定める義務に違反し、主務大臣の命令にも違反した場合には、刑事罰として 6 ヶ月以下の懲役または 30 万円以下の罰金が課せられる場合がある。

ISMS と同様に、サイバーセキュリティへ対策するためには、一般的に個人情報保護管理体制が定める1年や半年の PDCA サイクルではなく、サイバー攻撃の情報収集や対策の改善などを短いサイクルで実施することが求められる。

出典:IPA「サイバーセキュリティ経営ガイドライン」



- ✓ **翔泳社「情報セキュリティマネジメント要点整理＆予想問題集」**
- ✓ **情報セキュリティマネジメント試験合格講座** http://rakupass.com/security/