インシデント・レスポンス・リテイナー・サービス

将来起こりうるセキュリティ・インシデントに備え、迅速かつ総合的なインシデント対応体制を確立、ビジネスへの影響を最小化

概要

強盗などの物理的な犯罪被害にあった場合には、警察に通報するのが一般的です。では、サイバー攻撃被害を受けた場合には、どう対応すればよいのでしょうか。多くの場合、捜査当局や官公庁による解決は期待できず、サイバー攻撃への対応に特化した民間のセキュリティ・コンサルティング企業に頼らざるを得ないのが現状です。しかし、このような事業者を事前に確保していない場合には、いざセキュリティ侵害が発生したとき、業者の選定や社内の承認の取り付け、契約の締結までに数日～数週間も待たされるケースが珍しくありません。この一連の作業に手間取っていると、調査が始まりもしないうちに、重要情報の窃取など深刻な被害が生じる恐れがあります。

インシデント・レスポンス・リテイナー・サービスとは

インシデント・レスポンス・リテイナー・サービスは、インシデント・レスポンス・サービスの契約条件を、セキュリティ・インシデントの発生前に交渉・合意するためのサービスです。あらかじめ契約条件を決定しておくと、いざという場合にインシデント・レスポンス・サービスを速やかに受けられます。このアプローチにより、インシデント対応に要する時間を大幅に短縮し、情報漏えいなどの被害を最小限に抑えられます。

インシデント・レスポンス・サービスの選定方法

どのようなサービスでも、実際に体験する前には正確な品質を判断できません。まだインシデント・レスポンス・サービスを受けた経験がない場合は、すでに利用したことのある同業他社に話を聞いてみるとよいでしょう。

ほとんどのリテイナー・サービスは、対応時間を保証しています。また、次のような質問に対する回答を検討すると、事業者の経験や能力を判断できます。

- 専任のインシデント対応チームを擁しているか。対応チームにはどのような実績があるか。
- 過去1年に対応したインシデントは何件か。どのようなタイプのインシデントに対応したか。
- マルウェア解析の担当者やインテリジェンスの専門家はいるか。
- 必要に応じて捜査当局と協働した経験はあるか。
- インシデント対応を終える際、攻撃者の排除が完了したことをどのようにして確認しているか。
- 発生が確認されたインシデントに対し、どのようなサービス・レベルを保証しているか。初動対応時に遠隔サポートを即時提供できるか。

MANDIANT
A FireEye® Company

ハイライト

- リテイナー・サービスがインシデントへの対応時間短縮に役立つ理由
- リテイナー・サービスの選定時に事業者に確認すべき事項
- 自社のビジネス・ニーズに最適なリテイナー・サービスを選定する方法

FireEye

自社のビジネスおよびセキュリティ要件に最適な事業者を選定

リテイナー契約は、お客様組織のニーズに合わせ、さまざまな形式で締結できます。あまり知られていませんが、プランによっては、無償での契約も可能です。一定時間分のサービス料金の事前支払いが必須のプランもありますが、有事の際の事務手続きの省略に主眼を置いた、初期投資不要のプランも用意されています。

自社に最適なリテイナー・サービスを判断するために考慮すべき事項を以下に示します。

- **予算：**最も一般的なタイプは、時間あたりの料金が定められ、一定時間分のサービス料金を事前に支払うプランです。インシデント・レスポンス・サービスの実施には、事前支払い分のサービス枠が使用され、一定時間を超えるサービスが必要になった場合は、事前に合意した時間あたりの料金でサービスを追加します。初期投資を望まない組織向けに、時間あたりの料金などの契約条件を事前に交渉・合意するだけのプランを用意している事業者も存在します。契約条件を事前に決定しておけば、いざセキュリティ侵害が発生したとき、事務手続きを省いて即座にサービスを受けることができます。
- **未消化のサービス時間：**すべての組織が深刻なセキュリティ侵害に見舞われるわけではありません。リテイナー・サービスを選定する際には、未消化のサービス時間の扱いについても考慮する必要があります。扱いはサービスによって異なり、未消化のサービス時間を予防的なインシデント・レスポンス・コンサルティング・サービスに利用できるケース、その事業者が提供する任意のセキュリティ・コンサルティング・サービスに利用できるケース、あるいは、契約期間の満了時に無効になるケースがあります。
- **対応時間：**ほとんどのリテイナー・サービスでは、24～48時間以内でのコンサルタントによるオンサイト対応が保証されています。事業者によっては、エージェントなどのテクノロジーをあらかじめお客様環境に導入し、コンサルタントの到着よりも早く調査を開始できるアプローチを採用している場合もあります。
- **契約期間と支払い条件：**多くのリテイナー・サービスは、契約期間が12か月、事前支払いが必須となっています。
- **サイバー保険：**広く普及しつつあるサイバー保険ですが、多くの保険が補償する範囲は、直接的なインシデント対応に要した費用に限定されます。また、多くの保険会社は、強固な予防的セキュリティ対策を講じている組織向けに、割安な保険料プランを用意しています。

Mandiantのインシデント・レスポンス・リテイナー・サービス

FireEyeグループのMandiantでは、次に示す3種類のリテイナー・サービスを提供しています。

ティア1：事前の費用は一切発生しません。サービス提供時の時間あたりの料金など、基本的な契約条件について交渉・合意します。

ティア2：一定時間分のサービス料金を事前に支払い、サービス・レベルが保証されます。

ティア3：予防サービスの料金を事前に支払い、サービス・レベルが保証されます。セキュリティ体制の事前の強化に焦点を当てたティアであるとともに、インシデント・レスポンス・サービスの時間あたりの料金は、3つのティア中で最も割安に設定されています。サイバー保険を契約中、または契約を検討中の組織に最適です。

インシデント・レスポンス・リテイナー・サービスの3つのティア

サービス	ティア1	ティア2	ティア3
IRサービスの契約条件を事前に交渉・合意	○	○	○
IRサービス・リクエストの24時間受付（直通電話またはEメール）	○	○	○
サービス・レベル（SLA）	ベスト・エフォート	○	○
割引料金でのサポート提供	–	時間あたりの料金を事前支払い + 随時追加	随時
Mandiantの予防サービス	–	未消化のリテイナー・サービス時間をMandiantサービスに利用可能[1]	リテイナー・サービス期間中に利用できる一連の予防サービスを購入
インシデント対応能力評価サービス	–	○	○
初期費用	–	選択したサポート時間による	選択したサービスによる

[1] 契約期間中の開始が必要

Mandiantコンサルティング・サービスの詳細については、以下のWebページをご覧ください。
www.FireEye.jp/services.html

ファイア・アイ株式会社 | 〒101-0054 東京都千代田区神田錦町3-22 テラススクエア8階 |
03－4577－4401 | Japan@fireeye.com | www.fireeye.jp
FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | +1 408 321 6300 |
877.FIREEYE (347.3393) | info@fireeye.com | www.FireEye.com