KASPERSKY lab

インシデントの調査サービス

www.kaspersky.co.jp

インシデントの調査サービス

デジタルフォレンジック - マルウェア分析

個別化されたインシデント調査を通じて、お客様が IT セキュリティインシデントを識別し、解決するための支援を行います。

企業ネットワークに対するサイバー攻撃の危険性は増す一方です。これらの攻撃は、犯罪者が選んだ標的に固有の脆弱性を悪用するように個別設計されており、しばしば、機密情報または知的財産の盗用や破棄、業務への悪影響、産業設備の損傷、金銭の盗難を引き起こします。

このように巧妙かつ周到な攻撃から企業を守る対策は、ますます複雑になっています。組織が実際に攻撃されているかどうかを明確にすることすら難しい場合もあります。

Kaspersky Lab のインシデント調査サービスは、脅威の詳しい分析を提供し、インシデントの解決に向けた適切な手順を助言することで、組織が防御戦略を策定できるように支援します。

サービスのメリット

Kaspersky Lab のインシデント調査サービスを利用すると、お客様は当面のセキュリティ問題を解決し、マルウェアの動作とそれによる結果を理解し、修正策をアドバイスできるようになります。また、以下の間接的なメリットもあります:

- サイバー感染によって生じる問題の解決コストを削減
- 感染した PC から流出する可能性のある機密情報の漏洩を阻止
- 感染による業務プロセスへの損害に起因する評判低下リスクを軽減
- 感染によって障害の発生した PC を正常な状態に復旧

Kaspersky Lab の調査は、デジタルフォレンジックとマルウェア分析に関する実用的な専門知識を持つ、経験豊かなアナリストによって実施されます。調査が完了すると、サイバー調査の完全な結果と修正手順の提案を含む詳細なレポートが提供されます。

デジタルフォレンジック

デジタルフォレンジックは、インシデントを詳しく描写することを目指した調査サービスです。前述のとおり、調査中に何らかのマルウェアが発見された場合、フォレンジックにマルウェア分析を含めることができます。Kaspersky Lab のエキスパートは、HDD イメージ、メモリダンプ、ネットワークトレースなどを使用して形跡をつなぎ合わせ、何が起きているのかを正確に理解します。その結果として、詳細なインシデントの説明を提供します。

お客様は最初に、形跡を集めてインシデントの概要をまとめます。Kaspersky Lab はインシデントの症状を分析し、マルウェアバイナリ(ある場合)を特定し、マルウェア分析を実施して、修正手順を含む詳細レポートを提供します。

マルウェア分析

マルウェア分析の目的は、組織を標的とした特定のマルウェアファイルの動作と目的を完全に理解することです。

Kaspersky Lab のエキスパートは、お客様から提供されたマルウェアサンプルを徹底的に分析し、以下の内容を含む詳細レポートを作成します:

- **サンプルの特性**:サンプルについて簡単に説明し、マルウェアの分類を決定します。
- **マルウェアの詳しい説明**:マルウェアサンプルの役割と脅威の動作および目的(IOCを含む)を詳しく分析し、その活動を無害化するために必要な情報を提供します。
- **修正シナリオ**:この種別の脅威から組織を完全に保護するための手段を提案します。

提供方法

Kaspersky Lab の調査サービスを利用する方法には以下があります:

- 合意済みのインシデント数に基づく定額制
- 個々のインシデントへの対応

KASPERSKY lab