**〜解説書〜**

　本ゲーム中で発生したインシデントについて各曜日で行うべき対応例を示します。理論的な最大の効果ポイントの合計は**1640ポイント**です。  
　下記対応例はあくまで、本ゲーム用に設定した仮想企業（別紙：仮想企業説明書参照）で発生したインシデントへの対応例です。実際には業種、企業規模、企業が提供するサービスの対象や内容、保有する情報、サイバー攻撃の種類や被害等の違いにより、適切な対応内容や優先順位は異なります。

　自組織において同様のインシデントが発生した際に適切に対応できる準備ができているか、下記対応例を参考に見直してみてはいかがでしょうか。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **月曜日** | **火曜日** | **水曜日** | **木曜日** |
| **実際の**  **状況** | PC1の利用者より不審なメールの添付ファイルを開いたとの連絡を受ける。  ===補足===  添付ファイルを開いたことにより、流行しているマルウェアの亜種に感染しました。 しかし、連絡を受けて即座に PC1をネットワークから遮断と隔離したこと、マルウェアが自己拡散するタイプではなかったことから、被害はPC1だけですみました。 | 外部機関より不審な通信が発生していると連絡を受ける。  ===補足===  すでにマルウェアに感染していたPC2(データベースメンテナンス用従業員端末)が社内に存在し、PC2が不審な通信を行なっていました。 ※ PC2は月曜日の不審なメールよりも前に、不審なメールの添付ファイルを開いており、その際にマルウェアに感染してしまっています。 | 不審な通信を行なっている端末（PC2）が特定され、顧客情報データベースにアクセスしていることが判明した。  ===補足===  PC2はデータベースメンテナンス用の端末だったので、PC2上に保存されていた管理者アカウントで、顧客情報データベースにアクセスされていました。 | 顧客情報データベースから10万件の個人情報が不正に取得され、PC2から外部に送信されている事が判明した。 また、外部機関からも個人情報漏洩の連絡を受ける。  ===補足===  データベースとPC2を詳細に調査した結果、顧客情報データベースから取得された10万件の個人情報が外部サーバーに送信されている事が判明しました。 |
| **行うべき対応例** | * D3 : PC1をネットワークから遮断・隔離 * D4 : 不審メールの調査 * D7 : PC1利用者へのヒアリング * D9 : 全従業員へ注意喚起 | * D11 : 外部セキュリティ機関へ相談 * D16 : 外部との通信ログ調査 | * D18 : CISOへ報告 * D23 : PC2の調査 * D25: データベースのアクセス権の見直し * D26 : データベースのログ調査 | * D31 : 法務部門へ相談 * D32 : お客様部門に今後の対応を相談 * D35 : 外部機関へ情報漏洩発生を報告 |
| **解説** | まずはマルウェア感染が疑われるPCのネットワーク遮断と隔離を行い、感染拡大を防ぐことが重要です。 その後、感染しているかどうかの調査を進めていきます。 また、従業員宛に不審メールが届いていることを社内周知して注意喚起することや、同様のメールを受信した従業員の把握、メールサーバー上で不審メール送信元アドレスの受信拒否設定も重要となります。 | 不審な通信を検知した場合はFirewallなどネットワーク機器のログを調査し、不審な通信をしていた端末を特定します。  また、当該端末のネットワーク遮断と隔離を行う事も重要です。 | マルウェアに感染したPCが個人情報や機密情報にアクセスしていた場合、実際にアクセスしていたデータやファイルを正確に特定し、被害状況を把握することが重要です。 また、インシデントレスポンスに慣れていない場合は外部のセキュリティ機関に相談するのも一つの手段です。JPCERT/CCなどのセキュリティ組織に相談すれば、インシデント対応方法や類似事例情報を教えてもらえます。 | 個人情報漏洩が起きた際には、社内関係各所へ報告することが必要になります。特に広報対応や法務対応が必要になることが多いため、広報部門や法務部門へ相談し、対応を検討しましょう。 また、監督省庁や個人情報保護委員会、警察などの社外への報告についても検討する必要があります。 |

■対応例で必要となる事前準備

* 不審メール対応方法の周知  
  社員が不審メールの添付ファイルを開いたり、リンクをクリックした際には、すぐに連絡をもらえるように、連絡先を周知しておきましょう。また、不審メールを開いた際の対応方法も周知しておきましょう。
* ネットワーク機器のログの設定  
  インシデント発生時に調査できるように、ネットワーク機器にあらかじめログ取得の設定をしておきましょう。
* 各種サーバーや従業員端末のログの設定  
  各種サーバーでアクセスログなどの設定をしておきましょう。  
  また従業員端末でも操作ログを取得する管理ソフトウェアの導入や、ファイル操作ログの設定などをしておきましょう。
* 関係部門との連絡体制の構築やインシデント対応手順書の作成  
  インシデント発生時にどのように対応するかあらかじめ決めておき、連絡体制やインシデント対応手順書としてまとめておきましょう。

■本ゲーム中で発生したインシデントの攻撃の流れ

下図は攻撃の流れを示したものです。メールの添付ファイルを開いただけでもマルウェアに感染し重要情報が窃取されてしまう可能性があります。

