Cybersecurity 向けの SAM

現在の世代の IT 環境は、クラウド ソリューション、モバイル デバイス、ソーシャル メディア、およびビッグ データという 4 大要因の影響を強く受けているため、これらの要因から、ほとんどの組織に変革が起きています。同時に、セキュリティ リスクと脅威の進化が急伸しています。IDC の調査によると、不正コピーされたソフトウェアに関連したマルウェアが原因で、2014 年の企業で 4,910 億ドルの費用がかかると推定されていました。

Cybersecurity Assessment エンゲージメント

マイクロソフトの Cybersecurity Assessment ソフトウェア資産管理 (SAM) エンゲージメントの重点は、お客様の環境に導入済みのソフトウェアを示して潜在的なリスク分野を特定することと、適切な IT ソフトウェア資産管理を実現できるようにサイバーセキュリティのプログラムとポリシーに関するガイダンスの概要を提供することです。

情報技術がかつてないほどの成長と革新を遂げ、ネットワーク接続がますます普及していることから、サイバーセキュリティに関する危険が増しています。

Cybersecurity Assessment エンゲージメントでは、お客様の組織におけるサイバーセキュリティ プログラム成熟度を、利用できるさまざまなモデルに照らして分析します。利用可能なモデルには、Council on Cyber Security が当初公開した Critical Security Controls (CSC: 重大なセキュリティ コントロール) や、マイクロソフトのサイバーセキュリティ成熟度モデルがあります。しかし、サイバーセキュリティ プログラム全体が効果を発揮するには、まずお客様の IT インフラストラクチャを理解し、IT インフラストラクチャがお客様の財務パートナー、サプライヤー、ベンダー、および顧客とどのようにつながっているかを理解する必要があります。以下に、発生している場合がある課題と、マイクロソフト SAM パートナーと Cybersecurity Assessment エンゲージメントについて協力することで得られるメリットの例を示します。

課題

最新の IT 環境は複雑になりがちなため、次のような理由からサイバーセキュリティ リスクが高まっています。

- ソフトウェアと更新プログラムが最新ではなく、サポート期限が終了している。
- Unknowingly downloading malware via 非正規デジタル ダウンロードや不明なベンダーからのオンライン購入によって、知らないうちにマルウェアをダウンロードしている。
- フラッシュ ドライブなどのリムーバル メディアを使用して、不適切なソフトウェアをインストールした。
- 承認されていない個人用デバイスで社内ネットワークにアクセスしている。
- 契約切れベンダーや解雇済み従業員が引き続き IT システムにアクセスできている。

機会

サイバーセキュリティに関するベスト プラクティスと手続きを導入すると、次の効果を得られます。

- ソフトウェア資産を安全に管理し、適切なサイバーセキュリティ対策を推進する。
- 脅威にすぐ対処可能な、弾力的で適応力のある IT インフラストラクチャを構築する。
- IT インフラストラクチャのセキュリティ保護によって、攻撃を効果的に防御できるようにします。
- データ損失、盗難による詐欺行為、従業員のダウンタイムを最小限に抑えることで、コストが削減され、効率性が向上します。

SAM エンゲージメントの活動内容

すべてのエンゲージメントは、お客様のインフラストラクチャ、ニーズ、および目標に応じて少しずつ異なっています。エンゲージメントは大きく分けて、計画、データ収集、データ分析、および最終プレゼンテーションの 4 つのフェーズで構成されています。

計画 – 計画フェーズでは、インフラストラクチャの背景情報をお客様から収集し、エンゲージメントの計画と目標を特定して、面会の日程を定め、データ収集と分析を開始するためにアクセスを調整します。

データ収集 – データ収集フェーズでは、インベントリー ツールを使用したソフトウェア資産の検出およびインベントリー作成に続いて、インベントリー データ、使用状況、および保有ライセンスのマッピングを作成します。また、Cybersecurity Assessment の推奨事項に関連するデータも収集します。すべての関連データや関連情報が収集されて完全で正確な分析が実行されるよう、主な関係者にアンケートやインタビューを実施する場合もあります。

データ分析 – データ分析フェーズでは、収集したすべての使用状況、保有ライセンス、導入、およびその他のデータに対するレビューと検証を行います。また、現在のサイバーセキュリティ状態を長期的な戦略や目標と比較した分析も実行します。分析フェーズでは、最終的にお客様の会社の潜在的な脆弱性とサイバーセキュリティ成熟度全体のアセスメントを行い、サイバーセキュリティ リスクを最小化する方法についての提案を提供します。

最終プレゼンテーション – SAM エンゲージメントの最後には、SAM パートナーが概要プレゼンテーションと一連の詳細レポートで、結果、提案内容、および次に行う手順について説明します。

Microsoft

データの収集と分析

インベントリー データを解釈する目的は、保護が必要な資産を検出し、リスクが生じる分野を特定することです。リスク分野には、金融パートナー、サプライ チェーン ベンダー、顧客などの外部システムとの接続が挙げられます。マイクロソフト認定 SAM パートナーが、改善の余地がある分野を特定し、一連の提案とプロセスを作成して、お客様の会社がソフトウェアへの投資配分を最適化してコンプライアンスを維持できるようにします。データの収集と分析には、次のように定義されるカテゴリが含まれます。

資産インベントリー

出発点として、SAM パートナーはお客様と連携して、適切なツールを選択し、インベントリー対象とするコンピューターの範囲を定義します。また、簡単にアクセスできるとは限らないデバイスやネットワークからデータを収集するために必要な、追加の手順を特定し、スキャンとデータ収集用の環境を準備します。使用するインベントリー ツールでは、サポート期間が終了したかサポートされていないソフトウェアを実行している可能性があるコンピューターが含まれるよう、幅広いデータ ポイントを収集する必要があります。インベントリーの作成が完了したら、SAM パートナーはお客様と連携して Cybersecurity Assessment を実施します。

データ解釈と技術要件

インベントリー データの収集結果を分析するには、全製品の導入、使用状況、および保有ライセンスを特定し、ドキュメントに記録します。パートナーは、さまざまなインベントリー ツールから収集したデータを統合し、このデータを重要情報にマップして、十分な情報に基づいた意思決定を支援します。たとえば、展開データを製品サポート ライフサイクルにマッピングすると、ソフトウェアのアップグレードが必要な時期がわかります。パートナーは、ソフトウェアとネットワーク アクセスが現在どのように監視されているかについても分析します。

導入に関する検討事項

続いて、パートナーはサイバーセキュリティ リスクを軽減するために実施が必要な、変更の余地を特定します。このカテゴリには、セキュリティ更新プログラムを定期的にインストールする、最新バージョンのウイルス対策ソフトウェアを使用することでソフトウェアを有効かつ最新の状態に保つ、職場での個人用デバイスの使用に関する監視と管理を開始するなどの活動が含まれます。

ライセンスに関する検討事項

パートナーは、お客様が現在の導入状況と使用状況に照らして適切なライセンスを取得していて正規のソフトウェアを使用しているかどうか、評価できるようにします。また、データ収集フェーズで収集した情報に基づいて、将来の目標に合った最適なライセンス オプションを提案します。

ポリシーの改善

サイバーセキュリティ プログラムの重要な側面には、ソフトウェアの不正コピー、マルウェア、情報の盗難、なりすまし詐欺などの形式のサイバー犯罪に関するポリシーを策定して、サイバー脅威によるリスクをプロアクティブに軽減することも挙げられます。SAM パートナーは、継続的なサイバーセキュリティぃｄげ プログラムを管理するポリシーとプロセスの策定と導入を支援します。

エンゲージメント提出書類

エンゲージメントの前には、お客様はパートナーから、エンゲージメントでの活動予定と作業内容を説明した確認開始書と完全な業務範囲記述書を受け取ります。エンゲージメントの最後には、次のようなレポートを受け取ります。

概要レポート	概要レポートには、エンゲージメントの適用範囲、結果、提案内容、および次に行うべき手順をまとめた概要が記載されています。
導入状況分析 (EDP)	EDP レポートには、お客様の IT インフラストラクチャに現在導入されているすべてのソフトウェアに関する詳細が記載されています。
ライセンス状況分析 (ELP)	ELP レポートには、導入ソフトウェアにマッピングされた保有ライセンスに関する詳細が記載され、お客様の組織におけるギャップや未使用ライセンスを明らかにします。
Cybersecurity Assessment レポート	このレポートには、全体的なサイバーセキュリティ成熟度のアセスメントと、サイバー脅威への対抗時にお客様の会社に生じるリスクを最小化するための提案が記載されています
ライセンス最適化提案レポート	このレポートでは、お客様の会社のマイクロソフト ライセンス プログラムとその構造を最適化する方法について提案します。このレポートには、お客様の会社における現在のライセンス プラクティスに関連したリスク、法的責任、および可能性と、ライセンスを適切に管理して将来のリスクを最小限に抑えたりサイバーセキュリティ戦略に合わせたりする方法についての提案内容が詳しく示されています。
データ追加活用法レポート	データ追加活用法レポートには、仮想化ロードマップの策定、クラウド移行計画の策定、SQL Workload アセスメントの実施など、他の目的に収集済みデータを使用する方法についての提案が記載されています。

ソフトウェア資産管理とは

http://www.microsoft.com/ja-jp/sam/overview.aspx

Microsoft