The bridge to possible

シスコ テクニカル セキュリティ アセスメント サービス

脅威を把握し組織のレジリエンスを確保

脅威を把握し組織のレジリエンスを確保

今日のネットワークは、数多くのアプリケーション、ワークロード、データがクラウドに移行され、急速に変化しています。しかも、モバイルワーカーが増え、ハイブリッドワークモデルの採用が世界中で進んでいることで、リモートからネットワークにアクセスするユーザーとデバイスの数は増加しています。こうしたさまざまな変化によって、組織は大きなセキュリティリスクにさらされています。リスクが増大すれば、レジリエンスを高めなければなりません。そのためには、どのような脅威に注意を払い、どのように投資して脅威に対処すべきでしょうか。

「Gartner 社の予測によると、継続的脅威露出管理 (CTEM) プログラムに基づいてセキュリティ投資を優先している組織は、2026 年の時点で、侵害の被害を受ける可能性が 3 分の 2 減少します」[1]

強力なセキュリティ態勢を維持し、セキュリティ問題を効果的に管理するには、実際に直面している脅威を把握すると同時に、定期的なテストによって緩和と検出のコントロールにギャップがないかを確認しなければなりません。また、インフラストラクチャ、デバイス、データ、従業員をハッカーから保護するには、それらすべてへの攻撃を検出し、制限し、対応できなければなりません。侵入が発生すると、復旧にかなりの時間がかかる可能性があり、経済的損失、データ侵害、評判の低下にもつながりかねません。

では、どうすれば、攻撃者の先手を打てるのでしょう。

そのためには、次のようなことができる必要があります。

- セキュリティ上の不完全な点やギャップを特定して、優先順位を付け、対処することで、自社の現状を把握する
- セキュリティコントロールの継続的なテストによって、セキュリティの正常性を常に最適化する
- 脅威への対応を評価することで、社内セキュリティチームを強化する

弱点の把握と、警戒を怠らないセキュリティ態勢の維持に必要なスキルセットを、自社で整えるのが難しい場合は、シスコがお手伝いします。

[1]Gartner 社、「Gartner Identifies the Top Cybersecurity Trends for 2023」

成果

- **認識：**脆弱性を評価し攻撃をシミュレーションすると、侵害に悪用される弱点が明確になるため、弱点への効果的な対処に必要な知識を得られます。
- **競争優位性：**適切なセキュリティ投資を行ったと思い込まず、データに基づき判断できる組織となり、投資の価値を測定できるようになります。
- **信頼性：**セキュリティ上の弱点を把握して対処することで、将来の攻撃を防止すると同時に、リスクを軽減し、規制当局からの罰金を避け、壊滅的な影響を及ぼしかねない侵害を防ぐことができます。
- **修復：**シスコは、お客様が、組織のレジリエンスに影響を与えかねない問題を迅速に解決できるよう支援します。
- **経験：**シスコは、35 年以上の経験に加え、セキュリティ専門家、サービス、製品に対して数々の賞を受けており、業界をリードするセキュリティの専門知識をお客様に提供しています。

シスコ テクニカル セキュリティ アセスメント サービス

サービスの詳細

脅威モデリング

脅威モデリングとは、ビジネス上の主要な機能、資産、データを確認するプロセスです。脅威インテリジェンス情報を使用して、サイバーインシデントが組織にどのような影響を及ぼすかのモデルを構築するものであり、緩和と検出のコントロール手法の特定を目的としています。脅威モデリングでは、一般に、その後、コントロールのギャップの評価を行います。これは、脅威モデルから「実装すべき」点を特定して、現時点でコントロール手法が存在しているかどうか、また想定どおりに機能しているかどうかを評価するものです。コントロールのギャップの評価は、セキュリティ アーキテクチャ アセスメント（緩和コントロール）、セキュリティ運用アセスメント（検出コントロール）、レッドチームなどの脅威シミュレーション（緩和および検出コントロールの両方）の形で行われます。

脅威緩和：セキュリティ アーキテクチャ アセスメント

実際に直面している脅威を把握したら、それらへの緩和策が適切で、想定どおりに機能していることを確認しなければなりません。シスコのセキュリティ アーキテクチャ アセスメントを導入すると、人、プロセス、テクノロジーに着目して、組織を総合的に評価できます。また、ネットワーク、クラウド、アプリケーション、IoT/OT アーキテクチャ、DevOps 機能といった、特定の機能を評価対象にすることも可能です。

脅威検出：セキュリティ運用アセスメント

直面する脅威をすべて緩和できるのが理想的です。しかし、脅威を検出できなければ、緩和策が想定どおりに機能しているかどうかを把握したり、そうでない場合の対処を行ったりはできません。シスコのセキュリティ運用アセスメントでは、お客様が直面している脅威に応じて検出機能を評価することで、対策上のギャップをすべて把握し、修復を行えるようにします。

脅威シミュレーション：レッドチーム

レッドチームによる脅威シミュレーションでは、実際のサイバー攻撃をモデル化しますが、これは、厳格な管理下で行われます。レッドチームによるシミュレーションにおいては、シスコのセキュリティ専門家が、最先端のハッキング手法、シスコ独自のツール、一般的なツールを使用して、関連する特定の脅威に対する防御をテストします。

サービスオプション

脅威への対応体制

- 脅威モデリング
- レッドチームによる脅威シミュレーション
- 侵入テスト(内部および外部ネットワーク、アプリケーションとクラウド、IoT/OT)

レジリエンスの確保

- セキュリティ アーキテクチャ アセスメント (ネットワーク、クラウド、アプリケーション、IoT/OT)
- デバイス設定およびビルドのレビュー
- DevOps セキュリティアセスメント
- セキュリティ運用アセスメント

ここでの目的は、実際の攻撃シナリオを再現することに加え、侵害の防止と抑制のために多層化されているセキュリティコントロールの有効性を評価し、弱点を特定することです。ここで得られた情報を活用すると、最も投資すべき対象を選択できるようになります。

侵入テスト

侵入テストでは、特定の資産やソリューションの弱点を評価し、多くの脆弱性スキャンで見逃されがちな脆弱性を明らかにします。侵入テストは、シナリオ駆動型のレッドチームのシミュレーションとは異なります。内部および外部ネットワーク侵入テストでは、特定のネットワークに対し、実務的なセキュリティ評価を行います。具体的には、価値の高いシステムやデータへのアクセスを試み、エクスプロイト可能な脆弱性を特定します。アプリケーション侵入テストでは、認証と承認を回避して基盤となるサーバーまたはデータベースへのアクセスを試行したり、インジェクションについての脆弱性のテストを行ったりすることで、アプリケーションのロジックや実装上の欠陥を特定します。IoT/OT 侵入テストでは、オペレーショナル テクノロジーの物理的な要素に重点を置きます。

シスコが選ばれる理由

シスコは、ネットワークセキュリティの分野を牽引しています。広範なトレーニングや、先進的なツールに加え、世界でもきわめて複雑なネットワークの設計、導入、保護を 35 年以上手がけてきた経験に基づいて、さまざまな手法を開発しており、こうした手法によって、お客様のインフラストラクチャを積極的に評価するとともに、お客様のビジネス目標に合ったセキュリティソリューションを設計し、セキュリティ上のギャップを解消しています。

次のステップ

詳細については、www.cisco.com/go/as にアクセスするか、シスコの営業担当者または認定パートナーにお問い合わせください。