SOPHOS

ソフォスアドバイザリーサービス

侵入テスト

実際の攻撃手法を再現したシミュレーションにより、
組織のセキュリティ防御を検証

独自の専門知識と豊富な経験、組織に合わせてカスタマイズした戦略を用いて脆弱性を特定し、セキュリティ防御を検証することで、セキュリティポスチャの強化、リスクの軽減、コンプライアンスの促進、そして運用効率の向上を図ります。

防御力とセキュリティポスチャのプロアクティブに強化

会社のリソースへの不正アクセスは、セキュリティの重大な問題であり、既存および新たな脆弱性の悪用、設定ミスの利用、不十分なセキュリティポリシーの隙を突くことで発生します。アプリケーション、ネットワーク、システムがセキュリティ上のリスクに対して脆弱でないことを検証することは、攻撃者に悪用される前に脆弱性を発見し、対応するうえで欠かせないステップです。脆弱性スキャンや評価は、ネットワークのギャップや脆弱性を特定するための「簡易的な」検査ですが、攻撃者がどのように環境へ侵入し、内部のシステムを足掛かりにしてネットワーク深部へ攻撃を進めるかを把握するには、より詳細なテストと検証が必要です。

ソフォスの侵入テストサービス

侵入テスト (ペネトレーションテスト、ペンテストとも呼ばれる) は、サイバーセキュリティの脆弱性を特定および実証し、「攻撃者が自社ネットワークに侵入できるか？」という問いに答える手法です。侵入テストは、実際のサイバー攻撃をシミュレーションすることで、システム、ネットワーク、アプリケーションの脆弱性を特定します。経験豊富なテスター (倫理的なハッカー) が脆弱性を利用して、攻撃者が何を達成できるかを実証します。

侵入テストには主に 2 つの種類があります。

- **外部侵入テスト：**Web サイト、VPN、公開型のサービスなど、インターネットからアクセス可能なシステムを中心にテストします。攻撃者が外部から境界を突破する状況をシミュレートします。
- **内部侵入テスト：**インサイダーの脅威やすでに境界を突破した攻撃者を想定し、内部ネットワークのシステム、アプリケーション、データを中心にテストします。

ソフォスは、すべての侵入テストを各組織の特性やニーズに応じてカスタマイズし、個別に実施しています。この手法は、業界トップクラスのセキュリティテスターによって実施されており、Sophos X-Ops 脅威インテリジェンスグループの独自の戦術とインテリジェンスを活用しています。このグループには、持続的標的型脅威（APT）や国家が支援する攻撃者に関するインテリジェンスと調査で高い評価を受けている Counter Threat Unit (CTU) が含まれています。

利点

- 高価値なシステムやリソースを対象に、内部・外部のセキュリティ対策を検証することで、防御体制の有効性を確認し、安心感を得ることができます。
- 顧客の環境に即した脅威モデルとコンテキストを踏まえ、具体的なテスト目標を達成します。
- 改善のための実用的な対策を受け取ることができます。
- Sophos X-Ops 脅威インテリジェンスグループから得られた最新のインテリジェンスに基づく洞察を提供します。
- 実際のリスクに基づいた侵害の可能性を評価します。

高度な攻撃をシミュレートして防御力をテストする

組織は、業界規制への準拠だけでなく、複雑化し進化するサイバーセキュリティの脅威環境をプロアクティブに管理するために、定期的に侵入テストを実施しています。定期的に侵入テストを実施することで、攻撃者が新たな脆弱性を突くために手法を進化させ続ける中でも、組織はその一歩先を行くことが可能になります。また、定期的なテストにより、インフラやアプリケーション、サードパーティーの統合製品の変更によって生じる弱点も発見できます。さらに、侵入テストは、現実的なリスクの認識、実行可能な改善策、セキュリティの強化を時間をかけて測定する手段を組織に提供します。

侵入テストの利点は以下の通りです。

- **プロアクティブなリスクの低減：**定期的に侵入テストを実施している組織は、セキュリティインシデントの発生件数が 50% 減少し、セキュリティインシデント管理にかかる総コストも 30% 削減されています [1]。
- **コンプライアンスの支援：**PCI DSS、ISO 27001 などの規制では、侵入テストの実施が求められることが多くあります。実際、73% の組織がコンプライアンス要件の遵守を、侵入テストを実施する動機として挙げています [2]。
- **コスト削減:**データ侵害の平均コストは 445 万ドル [3] ですが、多くの脆弱性は、侵入テストによってそのごく一部のコストで事前に発見・対処することが可能です。
- **顧客からの信頼：**65% の消費者が、強固なサイバーセキュリティ対策を実施している企業をより信頼すると回答しています [4]。

サービスの特徴

- ビジネスクリティカルなデータが存在する対象システムのレビューなど、カスタマイズされた作業範囲の決定。
- 詳細な調査結果と経営幹部向けのサマリーを含む最終レポートの提供。
- 外部侵入テスト、内部侵入テスト、特定のユースケースに合わせた複合的な脅威シナリオを作成可能。
- サイバー攻撃者が使用する戦術をテスターが手動で実行

レポートの内容

エグゼクティブサマリー：技術的なスキルを持たない関係者 (経営幹部、監査人、取締役会、その他の重要な関係者) 向けの内容。

詳細な調査結果：技術スタッフ向けに、詳細な調査結果と推奨事項が記載された内容。

実施方法：調査の範囲と実施されたテスト活動を定義します。

説明文：テスターが調査の目的を達成するために行った一連の行動を明確に説明することで、複合的な脅威や段階的に進行する攻撃の全体像を把握しやすくします。

推奨事項：詳細な調査結果、参照のための Web ページリンク、改善やリスク低減のための推奨事項を記載しています。テスターは、必要に応じて調査結果の根拠を提示し、可能であれば一般に公開されているツールを使って同様の結果が再現できるように、十分な情報も併せて提供します。

その他のサイバーセキュリティテストサービス

1 つの評価や手法だけでは、組織のセキュリティポスチャを包括的に把握することはできません。各攻撃シミュレーションテストに固有の目的と許容されるリスクレベルがあります。ソフォスは、顧客と協力して、セキュリティポスチャやセキュリティ対策を評価し、脆弱性を特定するために、どの評価や手法の組み合わせを使用すべきかを検討します。

詳細情報:
sophos.com/ja-jp/advisory-services

[1]Ponemon Institute [2]SANS Institute [3]IBM [4]PwC

ソフォス株式会社
Email: JP_Presales@sophos.co.jp

2025-06-05 BREN (MP)