DATA SHEET

FortiGuard ペネトレーションテストサービス

リモートペネトレーションテスト

フォーティネットは、脅威分析と脆弱性研究の長年にわたる経験を基にした独自のペネトレーションテストサービスの提供を開始しました。

15 年以上にわたり、FortiGuard はそのスキルの向上とツールの改良に取り組み、世界有数のサイバーセキュリティ研究機関の一つに数えられるようになりました。数百名のスペシャリストが在籍する FortiGuard は、他のセキュリティベンダーを圧倒する 800 以上のゼロデイを発見し、業界において高い評価を得ています。

脆弱性の発見

ネットワークや重要なホストにおける現在のセキュリティの不備を理解し、それらを保護するために適切なアクションを実行します。

減災のアドバイスの提供

経験豊富なセキュリティエキスパートから、問題解決の手順が提供されます。

インシデントへのレスポンステスト

セキュリティチームを整備し、実際の脅威に対する既存の監視ツールの有効性をテストします。

調査方法

- これらのサービスでは、OWASP（Open Web Application Security Project）を活用してお客様のセキュリティ制御に関する一連の技術評価を実施し、コンピュータハードウェアのインフラストラクチャとソフトウェアアプリケーションの弱点を判定します。
- FortiGuardペネトレーションテストチームは、業界で活用されている自動化ツールを使用してお客様のネットワークで意図せず公開されているサービスを発見するとともに、実世界における攻撃者の方法論も適用して特定の標的における未知の脆弱性を発見します。

サービスの主な内容

FortiGuard ペネトレーションテストチームは、ネットワークに存在するセキュリティの不備を理解したいと考える企業に対し、リモートによる下記の脆弱性評価 / ペネトレーションテストサービスを提供します。このサービスでは、通常自動および手作業による評価手法が求められる、お客様の資産に対するいくつかの技術テストがリモートから実施されます。

外部の脆弱性評価

外部の視点から、インターネットに対するシステムの脆弱性を特定し、評価します。この評価では、依頼元企業の外部への公開状態などが検証されます。

Web アプリケーションペネトレーションテスト

不正アクセス、権限昇格、エクスプロイト、データの漏洩など、Web アプリケーションのリスクによる影響を評価します。Web アプリケーションの脆弱性は、「OWASP Top 10 Application Security Risks」に準拠した評価が実施されます。アプリケーションにおける認証については、お客様から提供された特定のアカウントを使用することができます。

内部の脆弱性評価

内部の視点から、システムの脆弱性を特定し、評価します。この評価では、お客様からリモートアクセスの許可、ならびに任意でネットワークアーキテクチャの開示をいただく必要があります。

モバイルアプリケーションの評価

不正アクセス、エクスプロイト、データの持ち出しなどの、モバイルアプリケーションのリスクによる影響を評価します。モバイルアプリケーションのテストは、「OWASP Top 10 Mobile Application Security Risks」に準拠した評価が実施されます。

サービス実施後の評価レポート

テクニカルフェーズの終了後、フォーティネットは脆弱性評価レポートを作成します。このレポートでは、評価の過程で発見された潜在的な問題とリスクの深刻度に基づくランキング、ならびに推奨される減災手順が提示されます。お客様は、Common Vulnerability Scoring System（CVSS）標準に基づいて提示された、High（高）、Medium（中）、Low（低）の深刻度に従って、問題に対する対策に取り組むことができます。

FORTINET
フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

DS-FSAS-R1-202003-R1