protiviti®
Global Business Consulting

アプリケーションとソフトウェアセキュリティ

ソフトウェアとアプリケーションのセキュリティ保障

リスク環境が拡大し続ける中、企業は次のような多くの課題に直面しています。

- 脆弱性の発見、修正、報告を行うためのセキュリティ専門人材の不足
- ソフトウェアとアプリケーションの脆弱性およびエクスプロイトの継続的な進化
- サードパーティSaaSやパッケージソフトウェアの導入に伴うリスクの顕在化
- コンプライアンス要件に基づくテストの実施だけでは、十分な保証レベルを確認できない可能性

プロティビティの支援内容

- **Web アプリケーションペネトレーションテスト**
- **モバイルアプリケーションペネトレーションテスト**
- **ソースコードレビュー**
- **シッククライアントペネトレーションテスト**
- **Web サービス /API ペネトレーションテスト**

> アプリケーションのセキュリティ脆弱性は、成功する攻撃チェーンにおける最初のステップとなることが増えており、近年発生した大規模なインシデントの背景にもなっています。
>
> —**Krissy Safi**
> Managing Director, Attack & Penetration

ビジネス成果

- 開発・利用するアプリケーションとソフトウェアに関連するリスクの完全な把握
- 社内開発アプリケーションがテストされ、脆弱性が正しく理解されていることへの確信
- ソフトウェアおよびアプリケーション開発プロセスがセキュアコーディング手法に準拠していることによる安心
- セキュリティ戦略の短期的および長期的改善を可能にする、明確かつ簡潔な修正アドバイス

アプリケーションとソフトウェアセキュリティ

プロティビティのアプローチと手法

Web アプリケーションペネトレーションテスト：プロティビティは、Web アプリケーションの脆弱性を特定するためのテストを実施します。自動化ツールを活用し、アプリケーション全体をクロール・マッピングすることで、脅威プロファイルとアプリケーション構造を理解し、動的アプリケーション・セキュリティ・テスト（DAST）を実施してビジネスロジックやセキュリティ制御のバイパスを試みます。OWASP トップ 10 を含む従来型の Web 脆弱性テストも対象となります。

モバイルアプリケーションペネトレーションテスト：プロティビティのモバイルアプリケーションアセスメントは 、デバイスレベルの制御、アプリケーションが使用する API や Web サービスを評価対象とします。実行時および保管時のデバイスとのインタアクションが安全かどうかを確認するため、モバイルデバイスの権限やファイル保護の分析を含みます。アプリケーションと基盤デバイス /OS とのインタアクションを分析し、セキュリティ上の懸念点や潜在的なビジネスインパクトを明らかにします。

ソースコードレビュー：プロティビティは、アプリケーション全体のデータフローを理解するための手動分析を実施します。認証、アクセス制御、入力検証、サニタイズ、外部コンポーネントとのインターフェースなどのセキュリティ制御を評価します。必要に応じ、アプリケーションが使用する API やライブラリ等の外部依存関係を評価し、さらなるセキュリティリスクをもたらさないことを確認します。

シッククライアントペネトレーションテスト：プロティビティは、ソースコードレビューを通じて静的解析を行い、必要に応じてローカルにインストールされたスタンドアロン実行ファイルのリバースエンジニアリングを実施します。動的解析フェーズでは、デバッグ、監視、トラフィックの遮断などの分析手段を行い、インストールされたアプリケーションとのインタアクションを通じて評価します。シッククライアントテストの性質上、分析対象に対するファジング等の攻撃実行のためにカスタムツールの開発が必要になる場合があります。

Web サービス / API ペネトレーションテスト:プロティビティは、自動スキャンとツールを用いて Web サービスのペネトレーションテストを実施します。このテストは API エンドポイントの脆弱性を発見するために設計されています。Web アプリケーションやモバイルアプリケーションが API からデータを取得する場合が多いため、これらのテストの一部として Web サービスペネトレーションテストが含まれることもよくあります。

ビジネス要件

グローバルなセキュリティ製品企業が SaaS 提供を拡大したことで、自社および顧客双方でリスクの増大が懸念されました。プロティビティは、新規および既存の提供サービスに対する一連のペネトレーションテストを実施するとともに、製品、企業、顧客を侵害しようとする攻撃者によって標的となりうる領域を特定するための包括的なアセスメントを実施しました。

ソリューションの提供

プロティビティは、お客様がサービスポートフォリオと組織全体のセキュリティ体制に自信を持てるようなテストプログラムを開発しました。お客様内部のサービスに関する専門家を活用することで、セットアップやデプロイメント支援の必要性をなくし、お客様のオーバーヘッドを削減しました。プロティビティのリソースは、新たに導入されたサービスやクラウドソリューションを含む、組織のさまざまな領域をカバーする包括的なセキュリティアセスメントを策定しました。

ビジネス成果

プロティビティは、新製品の脆弱性をリリース前に特定し、修正した上でのサービス開始を可能にしました。お客様はまた、既存製品に関連するリスクや、軽微に見える脆弱性が現実世界の脅威と同様に連鎖して悪用される可能性について、組織レベルでの深い洞察を得ました。

プロティビティ LLC　*protiviti.jp*

東京：東京都千代田区大手町 2-6-4 TOKYO TORCH 常盤橋タワー 24F　**大阪**：大阪府大阪市北区梅田 3-2-123 イノゲート大阪 9F

Protiviti、Protiviti ロゴは、Protiviti Inc. の米国ならびにその他の国における商標または登録商標です。その他の記載されている会社名・製品名は各社の登録商標です。
© 2025 Protiviti Inc. All rights reserved. 複写禁、転載禁

protiviti®