セキュリティツール診断
サービス紹介資料

情報セキュリティ株式会社

セキュリティツール診断内容概要

本セキュリティ脆弱性診断を実施することで、以下の項目を確認することが可能です。

1 プラットフォーム・ミドルウェア脆弱性

- ソフトウェア、仮想アプライアンスまたはハードウェアアプライアンスに対するセキュリティ脆弱性
- 日々のアップデートを行うことにより、61,000を超える項目を確認

2 WEBアプリケーション脆弱性

- 読み取ったHTTPリクエストやレスポンスの内容をチェックしWEBアプリケーションに対するセキュリティ脆弱性
- SQL InjectionやCross Site Scriptingなどの脆弱性が存在するかどうか確認

プラットフォーム・ミドルウェア脆弱性スキャナ について

プラットフォーム・ミドルウェア脆弱性スキャナは、以下のTenable社「Nessus」を用いてセキュリティ診断を実施いたします。

脆弱性スキャニングとコンフィグレーション監査

- ソフトウェア、仮想アプライアンスまたはハードウェアアプライアンスに対するセキュリティ脆弱性調査
- 日々のアップデートの61,000を超えるセキュリティチェックが高速動作
- パッチ監査
- コンフィグレーション監査
- ウェブアプリケーション監査
- データベース監査
- コンプライアンス監査（内部または産業標準）
- 悪意あるエレメントの発見
- ボットネット検出

Nessus vulnerability scanner

※Tenable社URL https://www.tenable.com/

アプリケーション脆弱性スキャナ について

アプリケーション脆弱性スキャナは、「WPScan」及び「OWASP ZAP」を用いてセキュリティ診断を行います。

WPScan

WordPress専用の脆弱性診断ツール

- コア、プラグイン、テーマに対する脆弱性診断の実行
- 登録ユーザ名の取得、任意の登録ユーザに対するブルートフォース攻撃の実行など

OWASP ZAP

WEBサーバの脆弱性を診断するためのペネトレーションテストツール

- 読み取ったHTTPリクエストやレスポンスの内容をチェックして脆弱性の可能性があるかどうかを判断
- Webアプリケーションへのリクエストを送ることにより、SQL InjectionやCross Site Scriptingなどの脆弱性が存在するかどうかのチェックを行う

弊社では、RFCに準拠したパケットを使用しシステムに負荷をかけないように慎重に実施いたします。通常はシステムには影響を与えることはありませんが、一部のシステムにおいては不安定になったり、システムが停止することがあります。

過去の脆弱性発見例

◎WordPressユーザ情報の一覧取得

問題点　：特定のリクエストによりWordpress上のユーザ名が取得可能となり、攻撃を受けやすくなった

対策方法：プラグインを導入し、スラッグを変更することにより、実際のログイン名から変更

◎脆弱性を突くことによるサイト情報の書き換え

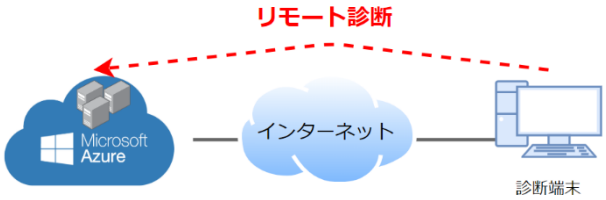
問題点　：某官公庁の外郭団体のサイトがSQLインジェクションの攻撃を受けたためサイトが改ざんされ信用問題に発展した

対策方法：Wordpress本体のバージョンアップを実施、かつ、
WAF（Siteguard lite)を導入し、不正通信は遮断

診断手法

ネットワーク機器、サーバ上のOS や各種アプリケーションに対して既知の脆弱性の存在を調査します。既知の攻撃や脆弱性を利用した攻撃を未然に防ぐことが可能です。

- **多角的な診断**
  複数の脆弱性診断ツール(Nessus等)と、自動診断ではできない不足部分に関しては豊富なセキュリティ診断実績を持つエンジニアによるマニュアル操作（Owasp ZAPもしくはBurp）を組み合わせて多角的に診断いたします。
- **診断結果レポートのご提供**
  項目別に詳細な診断結果をレポートにて提供し、問題を見える化します。
- **診断後のアフターフォロー**
  お客様のサーバに対して是正対策をご提案させて頂き、必要に応じて対策及びセキュリティサービスを実施いたします。

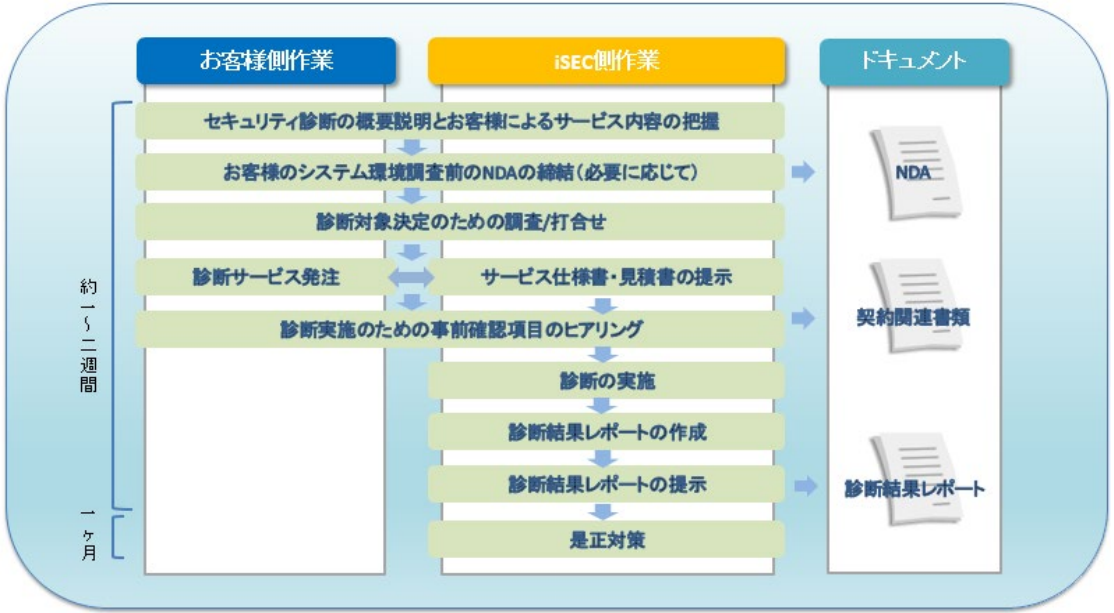


※ブラックボックス型による診断を想定

約1030サイト
（2019年単年度診断実績）

【参考】セキュリティ診断実施例とレポートサンプル

セキュリティ診断実施例



報告書サンプル