脅威モデリング

アプリケーションの設計に潜む弱点を洗い出します

脅威モデリングは、危害を生じうるタイプの脅威エージェントを特定するとともに、悪意あるハッカーの視点に立ち、ハッカーがどれだけの損害を与えることができるかを明らかにします。一般的に列挙されている攻撃以外に、新種の攻撃やその他の手法では考慮されることのない攻撃まで視野を広げて考えます。

回避すべき 4 つのセキュリティ・シンクホール

脅威モデリングでは、以下のものを特定してアタック・サーフェス全体を定義します。

- **一般的な攻撃では判断できない脅威**
  すべてのシステムにとって、一般的な攻撃が必ずしもリスクになるわけではありません。脅威モデルは、個々のシステム構成に特有の攻撃を特定します。
- **脅威エージェントがアーキテクチャのどこに存在するか**
  脅威エージェントの場所、動機、スキル、能力をモデル化し、潜在的な攻撃者がシステム・アーキテクチャのどの部分に存在するかを特定します。
- **トップ N リスト、攻撃者、最悪シナリオ**
  脅威モデルを作成・更新し、アプリケーションに関係する内部および外部の攻撃者に対して常に先手を打ったフレームワークを維持します。
- **追加の保護が必要なコンポーネント**
  資産、脅威エージェント、セキュリティ対策を明らかにし、どのコンポーネントが最も攻撃の標的になりやすいかを突き止めます。

組織のニーズに合わせてアプローチを調整

リスク・プロファイルとリスク許容度は組織ごとに異なるため、組織のニーズと予算に合わせてアプローチを調整します。ブラック・ダックの全体的な視野に立った脅威モデリング・アプローチは、2 つの基本的なステップで構成されます。

1. システムの主要なソフトウェア・コンポーネント、セキュリティ対策、資産、信頼境界線のレビューを実施します。
2. 次に、既存の対抗策に対するこれらの脅威をモデル化し、潜在的な結果を評価します。

ハッカーを食い止める最良の方法は、ハッカーの視点で考えること

脅威モデリングの 6 つの利点

セキュリティに真剣に取り組み、以下の目標を達成しようとするなら、脅威モデリングが最も効果的な手段です。

- コード実装前の SDLC の早期段階で問題を検出する
- 従来のテスト手法やコード・レビューでは見落としがちな設計上の欠陥を特定する
- その他の手法では考慮されることのない新種の攻撃を評価する
- テストとコード・レビューの対象を絞り込むことにより、テスト予算を最大化する
- 要件定義プロセスの穴を特定する
- ソフトウェアのリリース前に問題を修正することにより、コードの修正を防ぎ、コストを削減する

脅威モデルには以下のものが含まれます。

- リスクに基づいて優先順位付けした資産
- 発現可能性に基づいて優先順位付けした脅威
- 最も可能性の高い攻撃
- 成功または失敗が予想される現在の対抗策
- 脅威を軽減するための緩和策

ブラック・ダックについて

ブラック・ダックは、業界で最も包括的かつ強力で信頼できるアプリケーション・セキュリティ・ソリューション・ポートフォリオを提供します。ブラック・ダックには、世界中の組織がソフトウェアを迅速に保護し、開発環境にセキュリティを効率的に統合し、新しいテクノロジーで安全に革新できるよう支援してきた比類なき実績があります。ソフトウェア・セキュリティのリーダー、専門家、イノベーターとして認められているブラック・ダックは、ソフトウェアの信頼を築くために必要な要素をすべて備えています。詳しくは www.blackduck.com/jp をご覧ください。

ブラック・ダック・ソフトウェア合同会社
www.blackduck.com/jp