HITACHI
Inspire the Next

MWS 2023 プレミーティング

セキュリティインシデントの現場で学んだ教訓

2023/06/29

株式会社 日立製作所
藤原将志

注：発表内容は個人の見解に基づくものであり、発表者が所属する組織の公式見解ではありません。

教訓１． 初動の切り分け判断では常に疑い、反証を検討

HITACHI
Inspire the Next

■初動対応での切り分け判断において

問題点： 誤解や思い込み → 断定的に判断 → 検討漏れ → 判断を誤る

〇攻撃者はこのような振る舞いをする（検討漏れ：システムの正常な動作でも同じ振る舞いをする） → 正常な動作であった場合

→ 過検知（フォールス・ポジティブ）

〇システムはこのような振る舞いをする（検討漏れ：攻撃者も攻撃をする際に同じ振る舞いをする） → 攻撃であった場合

→ 検知漏れ（フォールス・ネガティブ）

例えば、

①プロキシログで、フィッシングサイトにアクセスしたことを検知した

②認証ログで、ユーザーがその数分後にパスワード変更していることを確認した

③「ユーザー自身が異変に気付いて、自分でパスワードを変更した」と判断した

→ それ以外の可能性はないか？ （例：攻撃者がパスワード変更した）

→ 例：追加で二要素認証ログ、接続元IPアドレスを確認する

教訓２．インシデントに備えてログ取得の設定を見直す

HITACHI
Inspire the Next

■セキュリティインシデントにおける証拠保全において

問題点：ログがない → 原因究明できない → 再発防止ができない

〇イベントログの保存期間が短い

・セキュリティのイベントログ（ログイン関連のログ）が数日分しか残ってない　→ いつから？どのアカウントで？接続元は？など有益な情報が得られない

※RDP（リモートデスクトップ）のログ（TerminalServices-LocalSessionManager, TerminalServices-RemoteConnectionManager）などで代替する。

〇ネットワークのログの保存期間が短い

・FWなどのアプライアンスで、機器内部に残っているログのみで、ログサーバーにログを転送＆保管してない → C2サーバーとの通信成否や転送量が不明

〇汚染された端末やマルウェアのファイルをすぐに消去してしまう

・マルウェアが検知された場合、ユーザー自身が危険だと判断して、証拠保全せず削除してしまう

・システムの再稼働を優先して、証拠保全せず、クリーンインストールしてしまう

教訓３． 脆弱性の修正確認は、修正前後の動作と修正方法を確認する

HITACHI
Inspire the Next

■脆弱性指摘の対応において
問題点：修正前の状態を記録してない → 正しく修正されているか確認できない

○WebサイトのSQLインジェクション/クロスサイトスクリプティング脆弱性の指摘
修正確認(ブラックボックスで)の依頼があった場合に備えて、

①修正前後での動作を比較するためには、修正前の動作を記録しておく

②ブラックボックスでは内部が見えない為、修正の方針、方法を確認する
例：SQLインジェクション → 静的プレースホルダで実装する
クロスサイトスクリプティング → エスケープ処理を行う

③同件見直しの観点(原因を分析する)：指摘箇所が一部であった場合、何故、指摘箇所のみに脆弱性が残存したのか？他にも同じ脆弱性が残存してないか？

教訓４． 調査報告は事実と推定(検証結果含)を分ける

HITACHI
Inspire the Next

■セキュリティインシデント調査報告書の作成において
問題点： 事実なのか推定なのか分からない → 信頼性、読み易さが低下

〇事実と推定を区別し、根拠や参照先を示す
・調査は、仮説立案と検証の繰り返し
・報告書は、論理的に説明し、事実に推定を加える。根拠や参照先を明記する

〇実機で検証する
・実際に再現テストを行って、推定した通りの動作になるか確認する
・OSのバージョンや設定によって、挙動やログの出力が変わる可能性がある

教訓５．日頃から手を動かし、実践的な対応スキルを高める

HITACHI
Inspire the Next

知っている　≠　実際にできる

知識として知っているだけでは、実際にインシデントが起こった時に対応できない

机上の理論だけでなく、実際に手を動かし、Try & Errorを繰り返すことにより、実践的な対応力を身に着ける