NEC

セキュリティの共通認識と開発･運用の現場

Dec.17 2008

NECネクサソリューションズ株式会社
セキュリティテクニカルセンター
中西 克彦（ Katsuhiko　Nakanishi ）

NEC

Chapter #01

Web Application

Webアプリケーションファイアウォール

WAFの効果と限界

- WAFとは？
  - リバースプロキシとして動き、HTTPリクエストを解析して、攻撃と判断すればWebサーバに渡さない。
  - Apache_modやISAPIフィルタのようなソフトウェアタイプもある。
- ホワイトリストとブラックリスト
- 難読化や文字コード問題
- やはり、プログラムでの対策が最も重要！！
- 高額な導入/運用負荷を強いる製品は避け、軽くてお手軽なものを選びましょう
- レポートで攻撃の特徴を掴む。Web-APに対する脅威を監視/管理しておく。

NEC

Chapter #02

セキュリティ診断

計画的なセキュリティ診断を

3ヶ年計画と5ヶ年計画

- セキュリティ診断が必要なのは理解しているが、何をどこまでやったらいいのか分からない。
  - システム全体（台数軸とレイヤ軸）の脆弱性検査は、コストもかかるし、指摘事項の対処も大変。

- 3ヶ年計画例 ⇒ ①サーバ　②クライアント ③アプリケーション
- 5ヶ年計画例 ⇒ ①外部公開サーバ ②その他サーバ ③アプリケーション ④サーバ ⑤クライアント

NEC

Chapter #03

セキュリティ製品・サービス

Bridging of the Developer & Operator

NEC

開発者と運用者の懸け橋

- セキュリティ製品やサービスを導入しても、使いこなせていない現状。運用しないと意味がない。

- セキュリティ製品を作る側は、機能強化や最新Exploitに対応するので精いっぱい。
- 運用する人の声を直接届けよう。そして、開発者の声に耳を傾けよう。
- 例①：WindowsUpdateにsecuniaの機能も入れて
- 例②：バージョンアップ前の評価を楽にするツールが欲しい。

NEC

Chapter #04

セキュリティに関する共通認識

common perceptions

NEC

全員が共通認識を持つ

- 要件定義といっても、ユーザだけでリスク分析できない。あなたがやろうとしていることはこれだけのリスクがある。と声を大にして言おう。

- 提示された予算で一部のセキュリティ対策ができない。⇒「じゃぁそこはお客さんの責任で」は×。特に運用面がお客様責任にされ、軽視されがち。
- 要件定義フェーズで、脅威を明確にする。開発/構築/運用時の対策を明確にする。それぞれのフェーズ責任者で認識合わせをする。

インシデント体験型 研修

- インシデント発生～調査～対策完了までを、CSIRTとして疑似体験する。グループワーク。
- SQLインジェクション（DBへのscriptタグ挿入型）により、Webサーバが攻撃を受け、そこにアクセスしたエンドユーザにウイルス感染するというストーリー
  - インシデント発生 ⇒ POC開設 ⇒ ヒアリング ⇒ 関係部門への依頼事項整理 ⇒ 対応プラン策定 ⇒ Webサーバのログ解析、ウイルスの解析（アンパック、サンドBOX解析等）⇒ ユーザへの報告書作成 ⇒ 防止ソリューションの提案　まで。
- 受講者の声。「疑似体験することで、気付きを得た」「自分のユーザが心配になりセキュリティ検査を提案することにした」「お客さんにセキュリティを語れるようになった」

NEC

まとめ

- 開発者と運用者が同じゴールを目指す
- お客様とベンダが共通認識を持つ（隠さない。バイアスかけない。）
- セキュリティは豪華一点主義では守りきれない。リスクがあるところには、多層防御で挑む
- 現状が把握できないことが一番の問題点。脅威を監視/管理して、脆弱点を把握しておく
- ディフェンス側の人間であるという意識を常にもっておく

NEC

Chapter #05

Security Operation

セキュリティオペレーション

セキュリティオペレーションとは？

1．「セキュリティオペレーション」は、いわゆるシステムオペレーションと何が違うのか。

2．SOCを取り巻く環境。複雑な攻撃手法。検知する仕組みを巧みに回避する攻撃者たち。

3．「セキュリティオペレーター」に求められるもの（役割、立ち位置、スキル）は何か。

4．課題は？今、足りてないこと。業界として取り組むべきこと。

ISOG-J Panel Discussion

END