SCIS2018

カンファレンス主催側からみた研究倫理

鵜飼裕司

株式会社ＦＦＲＩ
http://www.ffri.jp

はじめに

- Responsible Disclosure に至る経緯とDiscloseに関する歴史

  - 黎明期におけるDisclose
  - 初期のセキュリティ産業界とDiscloseの実態
  - 脆弱性情報の「価値の認知」とDiscloseの変化
  - セキュリティ産業界における脆弱性情報のDiscloseの現状

- CODEBLUEでの取り組み

黎明期におけるDisclose

- Full Disclosureが基本

  - 90年代後半
  - 大量の致命的な脆弱性
  - 情報が少ない
  - ベンダーは「保身」
  - Bugtraqや様々なフォーラムで「暴露」
  - ハッカー文化の台頭
  - 被害も拡大
  - 対策のコミットと引き換えにResponse Disclosureが台頭

初期のセキュリティ産業界とDiscloseの実態

- 2000年代前半

  - 脆弱性の発見技術の飛躍的な進展
    (IDA等のツールやFuzzing、解析手法等の整備)

  - 大量の脆弱性発見
  - 北米では「マーケティングツール」化
  - Responsible Disclosure / Coordinated Disclosureがメイン
  - pocは非公開の流れに

- BlackHat含む様々なカンファレンスで稀に0-dayの公開等が発生

  - 発表者のリスク
  - 主催者側のリスク

脆弱性情報の「価値の認知」とDiscloseの変化

- 2000年代後半

  - 脆弱性発見の高コスト化
  - アンダーグラウンドビジネスの台頭
  - 脆弱性情報の売却モデルの台頭
  - マーケティングツールとしては低コストなIoT関連に移行

セキュリティ産業界における脆弱性情報のDiscloseの現状

- 多くの国内セキュリティベンダーは脆弱性発見に注力しない

  - 価値の相対的低下
    - 効果に対するリスクとコストの問題

  - 案件としてのニーズは今でも大きい
    当然一般公開はしない

- セキュリティベンダーを中心としたセキュリティ産業界では、

  - Responsible Disclosure / Coordinated Disclosure
  - 脆弱発見を積極的に行わない
  - 偶発的に見つかった脆弱性は報告しない
  - 案件としての実施

  ブランディング、マーケティング的な視点で社会規範が守られる

  脆弱性公開で社会的非難を受けるリスクを取る理由はほぼ無い

CODEBLUEでの取り組み

- グローバルカンファレンスという事もあり「際どい」ものも多数投稿
- Abstractと発表資料の事前確認を入念に行っている
- 複数のReviewerが一つのCFPのレビューを担当してリスクヘッジ
- Abstractで懸念のあるものは本人に直接確認後、発表資料も確認

NG発表

- 0-dayおよびそれに類する情報
- 0-dayでなくとも、この発表がきっかけで大きな被害が発生する可能性があるもの
- ベンダーに対する信用棄損等が疑われるもの
- その他、CODEBLUEに対する法的責任や同義的責任の追及に至る可能性があると判断されるもの

CODEBLUEと主催者に対するリスクヘッジ

まとめ

- 脆弱性情報公開に対する「倫理」は「社会的コンセンサス」？
- 民間企業や産業界中心のセキュリティカンファレンスで適切な合意形成を目指すのはハードルが高い