2015/08/25

私情協大学セキュリティ研究講習会「イントロダクション」

私情協大学セキュリティ研究講習会運営委員会

1. ２つのインシデント事例から

① 2015 年度の事例

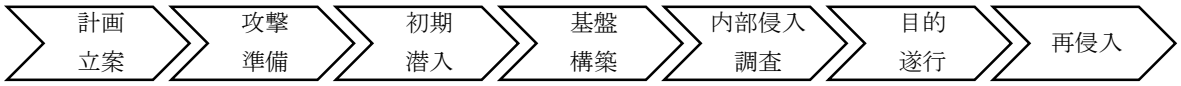
ｉ）日本年金機構からの基礎年金番号情報の流出

ii）大学からの個人情報流出

② 標的型サイバー攻撃の定義

実在する人物名を騙ったり、業務に関係した内容を装ったりするなど巧妙な手口で**遠隔操作**可能なマルウェアを感染させ、情報窃取などを遂行するサイバー攻撃の一種。**攻撃者**によってマルウェアの操作がなされる点が特徴。メールに添付されたマルウェアに感染することが発端となることが多い。

③ 標的型サイバー攻撃の段階



④　標的型サイバー攻撃の被害特徴

ｉ）マルウェア感染の手法は様々（メール添付ファイル、配布 DVD、USB メモリ）

ii）攻撃者からマルウェアへの操作命令がなされる

iii）攻撃者はマルウェアを拡散させる

iv）被害は外部通知で発覚することも多い

2. 今回の講習（総合演習１・2）で扱うインシデントモデル

① SJK 大学　学生 4000 人　教職員 300 人

② SJK 大学で発生したインシデント例

ｉ）学外のある PC が乗っ取られて C&C サーバが構築され、その PC と学内の端末間との通信ログが発見された。研究データらしきファイルも保存されていた。外部通知による発覚例。

ii）学内の職員から、「不審なメールの添付ファイルを開いてしまい、マルウェア感染した疑いがある」、と報告を受けた。被害状況の調査と対応が必要。内部通知による発覚例。

iii）マスコミより、学内設置されている複合機（プリンタ）の管理画面にインターネット側から接続できデフォルトパスワードで閲覧可能な状態にある、との指摘を受けた。外部通知による発覚例。

	漏洩状況	漏洩源	発覚
①	研究データ	教員所有PC	外部通知
②	ー	事務局所有PC	内部通知
③	印刷ログ	複合機（プリンタ）	マスコミ

③ 大学執行部に向けて

サイバー攻撃の脅威・危機意識の共有化、学内ルール構築、委員会主導の防御体制と点検、模擬訓練

3. 標的型サイバー攻撃の被害調査は大変！

① 被害調査

ⅰ）メモリや HDD のデータ保全

ⅱ）ファイルやレジストリの変更記録の収集

ⅲ）不審プロセスの洗い出し → 不審プロセスの通信先の調査

ⅳ）不審プロセスを起動したアカウントの洗い出し → 不審アカウントの操作記録の調査

② 被害調査のゴール

被害範囲の特定、侵入経路の特定、窃取データの特定

※ 被害調査のためには、メモリ上の情報が有益 → 「マルウェア感染した PC の電源は切らない」ことが求められる。

4. 今回の講習（総合演習 1）における標的型サイバー攻撃への対応フロー

① ネットワーク・システムの把握

② 被害範囲の予想

③ 報告・連絡・協議

④ 感染拡大防止・緊急対応

⑤ 警察への連絡・セキュリティベンダーへの依頼

⑥ 大学執行部への提言

5. 講習の流れ