情報通信の基礎知識

情報セキュリティマネジメント

東京デザインテクノロジーセンター専門学校　講師　石川敢也

Computer System

- 情報セキュリティマネジメント
  - 情報セキュリティの確保に、
    組織的・体系的に取り組むこと。
- 内容
  - 情報セキュリティポリシ、ISMS
  - リスクマネジメント、リスクアセスメント
  - マルウェア、ボット、キーロガー
  - DoS攻撃、マクロウイルス、トロイの木馬
  - ランサムウェア、ソーシャルエンジニアリング
  - SQLインジェクション、クロスサイトスクリプティング

Confidentiality／Integrity／Availability

- 情報セキュリティ
  - 「情報の機密性、完全性、可用性を維持すること」（JIS Q 27002／ISO/IEC 27002）
- 情報セキュリティの3要素
  - 機密性（Confidentiality）
    - 許可された正規のユーザだけがアクセスできる状態を確保すること。
  - 完全性（Integrity）
    - 情報が正確であり、改ざんされたり破壊されたりしていないこと。
  - 可用性（Availability）
    - 認められた利用者が、必要なときに利用できること

Information Security Policy

- 情報セキュリティポリシ
  - 企業や組織の情報セキュリティに関する取組みを包括的に規定した文書。情報セキュリティ基本方針、情報セキュリティ対策基準で構成される。
- 情報セキュリティ基本方針（狭義のポリシ）
  - どのようにして情報を守るかという基本的な考え方。
- 情報セキュリティ対策基準（スタンダード）
  - 基本方針を実現するための基準を定めたもの。
- 情報セキュリティ実施手順（プロシージャ）
  - セキュリティ確保の具体的な手順を定めたもの。

Information Security Management System

- ISMS
  - ISO/IEC 27001 (JIS Q 27001)
  - 情報セキュリティマネジメントシステムの管理・運用に関する仕組み。
  - 保護すべき情報資産を特定し、リスク対策を決める。
- ISMS におけるセキュリティリスクへの 4 つの対応
  - 移転〔________________________________〕
  - 回避〔________________________________〕
  - 受容〔________________________________〕
  - 低減〔________________________________〕

Risk Management

- リスクマネジメント
  - リスクについて、組織を指揮統制するためのプロセス。
  - リスクマネジメントは一般的に下記の手順を取る。
    - リ スクの特定
    - リスクの大きさの算定
    - リスクの大きさの評価
    - 対策の導入手順
- リスクアセスメント(Risk Assessment)
  - 守るべき情報資産で発生する可能性のある脅威と、発生確率や発生した場合の影響度等を評価する方法。

Malware

- マルウェア
  - ウイルスやスパイウェアなど、悪意のあるソフトウェアの総称。
- ボット
  - ネットワークを介して、他人の PC を自由に操ったり、パスワードなど重要な情報を盗んだりするプログラム。
- クラッキング（Cracking）
  - 悪意をもってコンピュータに侵入し、データを盗み見たり破壊したりする行為。
- IPスプーフィング（Spoofing）
  - 偽の送信元 IP アドレスをもったパケットを送る不正行為。

Buffer Over Flow

- バッファオーバフロー
  - プログラムが用意している入力用のデータ領域を超えるサイズのデータを入力することで、想定外の動作をさせる。
- バックドア
  - サーバに設けられた、不正侵入を行うための通信経路。
- キーロガー（Key Logger）
  - キーボード入力を記録する仕組み。
- ポートスキャン
  - TCP/IP のプロトコルのポート番号を順番に変えながらサーバにアクセスし、侵入口と成り得る脆弱なポートがないかどうかを調べる攻撃。

Social Engineering

- ウォードライビング（War Driving）
  - 無線LANの電波を検知できるPCを持って街中を移動し、不正に利用が可能なアクセスポイントを見つけ出す行為。
- ソーシャルエンジニアリング
  - 巧妙な話術や盗み見などによって、パスワードなどのセキュリティ上重要な情報を入手したり、システムに侵入しようとしたりする攻撃。
  - 本来は「社会工学」という学問を意味する用語。
- ワンクリック詐欺
  - サイトの閲覧や画像のクリックだけで料金を請求する詐欺。

Trojan Horse

- トロイの木馬
  - 利用者に有用なソフトウェアと見せかけて、利用者のコンピュータに侵入しようとする攻撃手法。
- マクロウイルス
  - 表計算ソフトなどの操作手順を記録する機能（マクロ）を不正に利用する攻撃。
- フィッシング
  - 電子メールなどを使って利用者を偽のサイトへ誘導し、個人情報などを取得しようとする攻撃手法。

Denial of Service

- DoS 攻撃
  - 特定のサーバに大量の接続要求を送り続けて、サーバが他の接続要求を受け付けることを妨害する攻撃。
- 総当たり攻撃
  - ブルートフォースアタック(Brute Force Attack)
  - 文字の組合せを、すべて試すことによって、パスワードを解読しようとする攻撃。
- 辞書攻撃
  - 辞書に載っている単語を入力してパスワードなどを、推測しようとする攻撃手法。

Watering Hole Attack

- 水飲み場型攻撃
  - 頻繁にアクセスする Web サイトに攻撃コードを埋め込み、アクセスしたときに不正行為が始まるように仕掛ける手法。
- ゼロデイ攻撃
  - ソフトウェアに脆弱性が存在することが判明したとき、その修正プログラムが提供される前に、攻撃してくる手法。
- パスワードリスト攻撃
  - どこかの Web サイトから流出した利用者 ID とパスワードのリストを用いて、他のWeb サイトにログインを試行する攻撃。

Ransomware

- ランサムウェア
  - 感染すると勝手にファイルやデータの暗号化などを行って、正常にデータにアクセスできないようにし、元に戻すための代金を利用者に要求するソフトウェア。

トレンドマイクロ社のWebサイトから引用

DNS Cache Poisoning

- キャッシュポイズニング
  - DNS(Domain Name System)キャッシュサーバに対して、偽の DNS 情報をキャッシュ として登録させることで、利用者を偽の Web サイトに誘導しようとする攻撃手法。

- SQLインジェクション
  - データベースに悪意のある問合せや操作を行う命令文を入力して、データベースのデータを改ざんしたり、不正に取得しようとする攻撃。

Cross Site Scripting

- クロスサイトスクリプティング
  - Web サイトの運営者が意図しないスクリプトを含むデータであっても、利用者のブラウザに送ってしまう脆弱性を利用する攻撃。

- セションハイジャック（Session Hijack）
  - サーバとクライアント間の正規のセッションに割り込んで、正規のクライアントに成りすますことで、サーバ内のデータを盗み出そうとする不正行為。

お疲れさまでした！