정보보호 개론

02. Threats & Vulnerability

Threats (1)

- 의도적인 위협(intentional threats)
  - 고의적인 침해 행위를 통해 부당한 정보 획득, 변조, 파괴를 시도하는 경우
  - 행위자 : 침입자(intruder), 크래커(cracker), 해커(hacker)
  - 적극적(active) 위협
    - 대상이 지정된 경우
      - 특정 시스템의 정보 삭제, 변조, 서비스 방해 등
    - 대상이 지정되지 않는 경우
      - 컴퓨터 바이러스, 인터넷 웜, 악성 코드
  - 소극적(passive) 위협

Threats (2)

- 비의도적인(accidental) 위협
  - 하드웨어나 소프트웨어의 장애나 사고
  - 자연 재해
  - 운영자의 실수

Vulnerability (1)

- 정보시스템의 취약성
  - 취약성(vulnerability) : 해당 정보시스템이 다양한 위협요소들 중 특별히 어떤 것들에게 취약한 부분이 노출되었는지를 나타내는 정도
  - 주변에 위협요소들은 많지만 충분한 대비가 되어있다면 취약성은 낮을 수 있음
  - 인적 취약성
    - 배경 조사 등의 선조사
    - 인적 관리
    - 주기적인 교육 및 관찰

Vulnerability (2)

- 정보시스템의 취약성(계속)
  - 물리적 취약성
    - 물리적 감시 체제
    - 시건 장치 및 경비
    - 개인 컴퓨터에 대한 잠금
    - 인증카드
  - 하드웨어 취약성
    - 정기 점검 및 교체
  - 소프트웨어 취약성
    - 버전 관리(업그레이드)
    - 보안 패치

Vulnerability (3)

- 정보시스템의 취약성(계속)
  - 자연적, 환경적 취약성
    - 먼지, 습도, 온도 대비 설비
  - 전자파 취약성
    - 전자파 방출로 인한 정보 유출 / 전자파로 인한 공격 방지
    - 전자파 방지 도료

Hacking (1)

- 정보보호 침해
  - 정보시스템에 대해 의도적인 위협요소를 발생시키는 행위
  - 프래커(phrecker) : 전화 해킹(프래킹)
  - 대상이 컴퓨터로 넘어가면서 해킹 등장
    - 1960년대 ~ 1970년대
      - 운영체제나 프로그래밍에 심취한 마니아
      - 정보통신 발전에 기여
    - 1980년대 이후
      - 불법 침입 및 정보 파괴, 변조, 유통에 관심
      - 범죄자로 전락

Hacking (2)

- 정보시스템 해킹
  - 시스템 해킹 시나리오
    - 시스템 잠입
      - 해당 목표 시스템의 계정과 암호 획득
        - 웹 서버나 네트워크의 취약점
        - 암호 크래킹
        - 사회공학
    - root 권한 획득
      - 해당 정보시스템의 취약성
      - 트로이 목마
    - 백도어(back door) 설치
      - 재침입을 위한 뒷문 설치
    - 구체적 공격
    - 침입 흔적(log) 제거
      - 관련 로그파일 변조

Hacking (3)

- 시스템 해킹 공격 유형
  - 소스 코드 취약점 활용
  - 시스템 운영 취약점 활용
    - IFS(Internal File Separator) 활용
    - race condition (경쟁조건) 활용
    - buffer overflow (버퍼 오버플로우) 활용
- 시스템 해킹에 대한 대응책
  - 보안 패치 설치
  - 기술 권고문 활용
  - 보안 관련 사용자 교육
  - 로그 및 보안 점검 도구 활용

Hacking (4)

- 네트워크 해킹 대표적인 공격기법
  - 서비스 방해(DoS; Denial of Service)
    - TCP SYN flooding
  - 패킷 스니핑(packet sniffing)
    - 엿보기
  - IP 스푸핑(IP spoofing)
- 네트워크 해킹에 대한 대응책
  - 암호화 기법 도입
  - 네트워크 취약성 점검 도구 활용
  - 패킷 모니터 활용
  - 네트워크 기반 IDS (Intrusion Detection System : 침입탐지 시스템)

Hacking (5)

- 해킹 발생시 조치 사항
  - 네트워크로부터 시스템 분리
  - 비정상적인 프로세스 종료
  - 전원 즉시 차단
    - 비정상 종료로 인한 피해 감수
  - 경미한 경우 한국인터넷진흥원의 기술적인 도움 요청
  - 수사가 필요한 경우 경찰청 사이버테러 대응센터나 대검찰청 컴퓨터수사과에 의뢰