정보보호

02 위험분석

1. 시스템의 위협요소 및 취약성 (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

1. 시스템의 위협요소 및 취약성 (2)

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

1. 시스템의 위협요소 및 취약성 (3)

- 정보시스템의 취약성 (계속)
  - 인적 취약성
    - 배경 조사 등의 선조사
    - 인적 관리
    - 주기적인 교육 및 관찰
  - 물리적 취약성
    - 물리적 감시 체제
    - 시건 장치 및 경비
    - 개인 컴퓨터에 대한 잠금
    - 인증카드

1. 시스템의 위협요소 및 취약성 (4)

- 정보시스템의 취약성 (계속)
  - 하드웨어 취약성
    - 정기 점검 및 교체
  - 소프트웨어 취약성
    - 버전 관리(업그레이드)
    - 보안 패치
  - 자연적, 환경적 취약성
    - 먼지, 습도, 온도 대비 설비
  - 전자파 취약성
    - 전자파 방출로 인한 정보 유출 / 전자파로 인한 공격 방지
    - 전자파 방지 도료

2. 해킹 기법과 대응 (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

구 분	해킹 기술	보안 기술
컴퓨터 시스템	시스템 해킹	시스템 보안 기술
네트워크 및 온라인	네트워크 해킹	네트워크 보안 기술

2. 해킹 기법과 대응 (2)

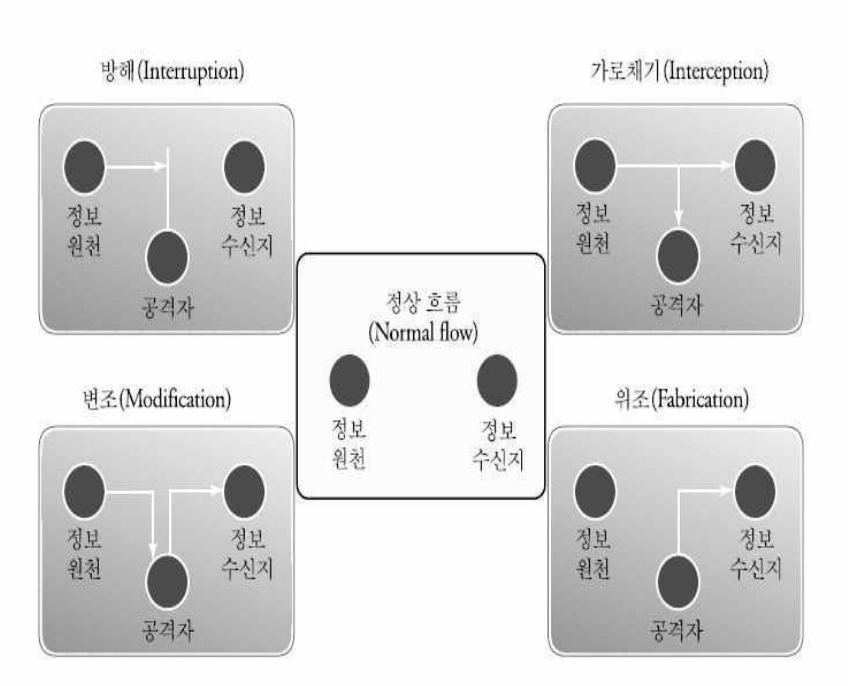
- 정보시스템 해킹
  - 시스템 해킹 시나리오
    - 시스템 잠입
      - 해당 목표 시스템의 계정과 암호 획득
        - 웹 서버나 네트워크의 취약점
        - 암호 크래킹
        - 사회공학
    - root 권한 획득
      - 해당 정보시스템의 취약성
      - 트로이 목마
    - 백도어(back door) 설치
      - 재침입을 위한 뒷문 설치
    - 구체적 공격
    - 침입 흔적(log) 제거
      - 관련 로그파일 변조

2. 해킹 기법과 대응 (3)

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

2. 해킹 기법과 대응 (4)

- 네트워크 해킹
  - 보안 침해 형태
    - 방해(interruption)
      - 가용성 침해
    - 가로채기(interception)
      - 기밀성 침해
    - 변조 (modification)
      - 무결성 침해
    - 위조(fabrication)
      - 무결성 침해



2. 해킹 기법과 대응 (5)

- 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
    - 스니핑 방지
  - 네트워크 취약성 점검 도구 활용
    - ISS
    - SATAN
  - 패킷 모니터 활용
    - TCPdump
    - Etherfind
  - 네트워크 기반 침입탐지 시스템(IDS: Intrusion Detection System)
    - gabriel
    - neowatcher

2. 해킹 기법과 대응 (6)

- 해킹 공격 감지
  - 보안 점검 사항 숙지 및 학습 필요
  - 프로세스 상태에 의한 공격 감지
    - 비정상적인 행동을 보이는 프로세스 실행 여부
      - 과도한 자원 점유
      - 잘 이용되지 않는 특별한 명령어 실행
      - 제어터미널이 없는 프로세스
  - 관리자나 사용자들로부터 통보
    - 공조체제에 의한 경보
    - 사용자의 민원
  - 로그 파일에 의한 공격 감지
    - 자원의 급격한 감소
    - 의심이 가는 접속 또는 ftp
    - 관리자 계정 로그인 시도
    - 로그 파일 삭제 또는 일부 훼손

2. 해킹 기법과 대응 (7)

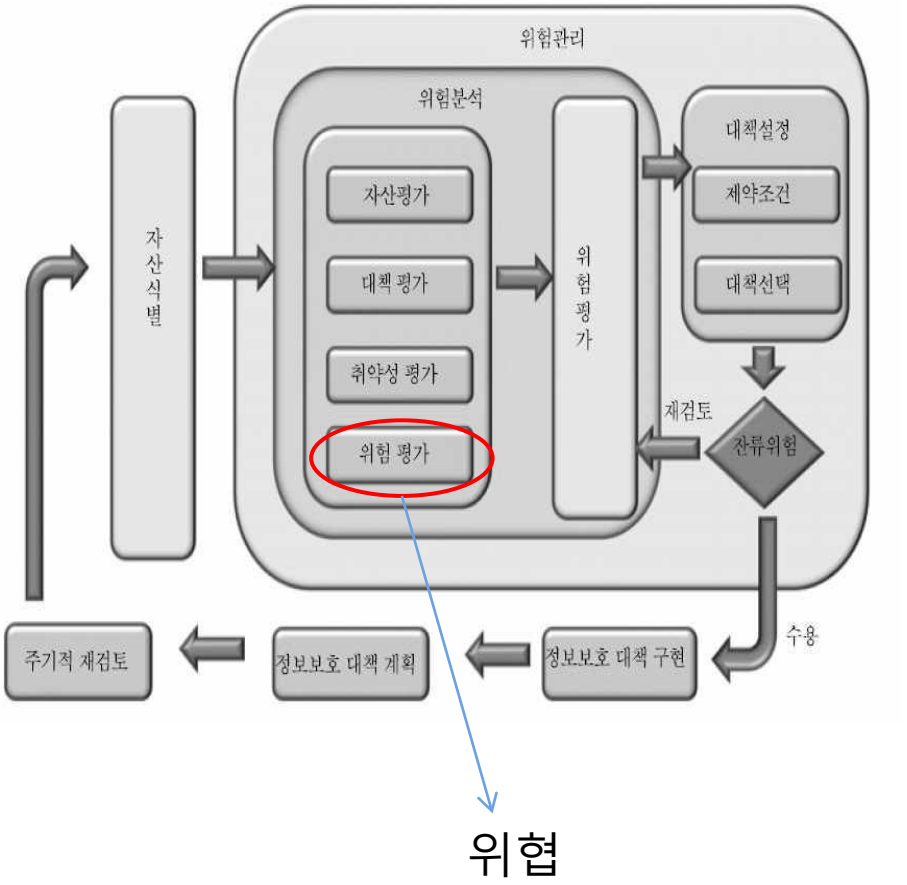
- 해킹 발생시 조치 사항
  - 네트워크로부터 시스템 분리
  - 비정상적인 프로세스 종료
  - 전원 즉시 차단
    - 비정상 종료로 인한 피해 감수
  - 경미한 경우 한국인터넷진흥원의 기술적인 도움 요청
  - 수사가 필요한 경우 경찰청 사이버테러 대응센터나 대검찰청 컴퓨터수사과에 의뢰

3. 위험 분석 관리 (1)

- 위험(Risk)
  - 비정상적인 일이 발생할 수 있는 가능성
- 위험분석(Risk Analysis)
  - 정보시스템 관련 자산의 기밀성, 무결성, 가용성 및 책임 추궁성(Accountability)에 영향을 미칠 수 있는 다양한 위협에 대해 정보시스템의 취약성을 인식하고, 이로 인해 예상되는 손실을 분석
- 위험 관리(Risk Management)
  - 조직 내 중요한 자산의 가치 및 민감도를 측정
  - 이에 대한 취약성 및 위협을 분석하여 위험의 정도를 측정
  - 조직에 요구되는 적절한 위험 수준으로 조정

3. 위험 분석 관리 (2)

- 위험관리 절차
  - 위험 분석
    - 위험 확인
    - 자산 가치 평가
    - 위협, 취약성
  - 위험 평가
    - 적절하고 적당한 보안 대책을 선정하였는지
    - 시스템과 자산이 노출된 위험을 평가하고 식별
  - 대책 설정
    - 허용 가능한 수준으로 위험을 줄이기 위한 대책 식별 및 선정



3. 위험 분석 관리 (3)

- 위험 분석
  - 정보자산(information assets) 분석
    - 정보자산 식별
      - 보호 받아야 하는 정보자산을 우선 구분
      - 자산의 형태와 소유자, 관리자, 특성 등을 고려한 정보 자산의 상세 목록 작성
    - 자산 가치 산정
      - 자산의 중요도를 파악하고 위협이 발생한 경우 입을 수 있는 피해 가치를 측정
      - 정량적 : 자산 도입 비용, 복구 비용, 교체 비용
      - 정성적 : 자산의 기여도, 영향을 받는 조직과 작업 수, 복구시간, 기타 요소

3. 위험 분석 관리 (4)

- 위험 분석 (계속)
  - 위협 분석
    - 위협(threat) : 정보, 자산, 서비스에 대한 불법적 유출과 파괴, 제거, 변경 등의 손실을 줄 수 있는 잠재적인 사건 또는 행위
    - 구분
      - 의도적 위협
        - 접근방식(mode) : 물리적 공격, 데이터 위변조, 악의적인 프로그램, 크래킹
        - 동기(motive): 사기, 스파이, 만행 등
      - 비의도적 위협
        - 자연재해
        - 인위적인 실수 또는 시스템 오류

3. 위험 분석 관리 (5)

- 위험 분석 (계속)
  - 취약성 분석과 대책
    - 취약성이 있더라도 위협이 없으면 손실로 이어지지 않는다.
    - 위협이 있더라도 취약성이 없으면 손실을 발생시키지 않는다.
    - 취약성 정의 (3가지)
      - 자산의 속성
      - 자산과 위협의 상관관계
      - 보호 대책의 미비
    - 위협으로부터 보호하기 위해 대책이 필요
      - 물리적 대책
        - 경비, 자물쇠, 통신망의 물리적 차단
      - 기술적 대책
        - 패스워드 등 각종 접근 제어, 침입차단 시스템
      - 절차적 대책
        - 출입자 기록부, 외부인 출입 규정
    - 기존에 수립된 대책에 대해 정상적인 작동 여부 확인
    - 새로운 보호 대책을 강구하는 경우 기존 대책과의 충돌 확인
    - 위험도와 비용 고려

3. 위험 분석 관리 (6)

- 위험 분석 (계속)
  - 위험분석
    - 위험 구분
      - 순수 위험
        - 이득 기회가 없는 것 -> 보안상 에 발생하는 위험
      - 투기 위험
        - 이득 기회가 있는 것
    - 위험은 위협과 자산의 함수 관계
    - 손실 발생 확률과 손실액 계산

3. 위험 분석 관리 (7)

- 위험분석방법론
  - 정량적/정성적 분석

	정량적 접근 방법	정성적 접근 방법
산출 개념	위험 발생 확률 × 손실 크기= 기대 위험 가치 분석	- 손실 크기를 화폐가치로 표현하기 어려움 - 위험 크기는 기술 변수로 표현
접근 유형	- 수학 공식 접근법 - 확률 분포 추정법 - 확률 지배 - 몬테카를로 시뮬레이션 - 과거 자료 분석법	- 델파이법 - 시나리오법 - 순위 결정법 - 퍼지 행렬법 - 질문서법
장 점	- 객관적인 평가 기준 적용 - 논리적으로 평가되어 이해가 쉬움 - 위험 관리 성능 평가 용이	- 가치 평가 및 계산이 필요 없음
단 점	- 많은 시간과 비용이 소요 - 자동화의 경우, 정확도의 변이	- 주관적인 평가 우려 - 결과의 이해가 어려움 - 위험 관리 성능 추적이 어려움

3. 위험 분석 관리 (8)

- 정량적 위험 분석
  - ALE(연간 예상 손실)
    - 단일 예상손실(SLE) = 자산가치 X 노출계수
    - 연간 예상손실(ALE) = 단일 예상손실 X 연간 발생률
  - 분석방법
    - 과거자료분석법
    - 수학공식접근법
    - 확률분포법
    - 점수법
- 정성적 위험 분석
  - 델파이법
    - 전문가 집단의 토론
  - 시나리오법
    - 발생 가능한 사건의 이론적인 추측
  - 순위결정법

정리

- 위협
- 취약점
- 위험
- 시스템 해킹 시나리오
- 시스템 해킹 대응책
- 네트워크 보안 침해 형태
- 네트워크 해킹 대응책
- 위험관리 및 절차
- 위험분석 절차
- 위험분석 방법론
- 용어 정리
  - 프래킹
  - 해킹
  - 크래킹
  - 스푸핑
  - 스니핑
  - 서비스 거부(DoS)