정보보호 개론

03. Threats & Vulnerability (2)

정보보호의 관리적 및 운영적 대책 (1)

- 조직체의 정보보호를 효과적으로 보장하기 위해
  - 다양한 기술적인 보호대책
  - 이들을 계획하고 설계하고 관리하기 위한 관리적 제도, 정책 및 절차 등의 확립 필요
- 정보보호 정책
  - 조직과 조직체의 임무에 관련
  - 임무 수행에 대한 위협에 기반을 둠
  - 보안 요구사항
    - 조직체의 정보 및 기타의 시스템 자원에 대하여 조직체가 요구하는 보호를 표현
- 절차, 표준, 지침
  - 정책이 조직 내에서 어떻게 구현되어야 하는지를 설명하는 자료
- 효과적인 정보보호정책 수립 -> 궁극적으로 더 나은 정보보호 프로그램 개발 및 구현 -> 시스템과 정보의 적절한 보호

정보보호의 관리적 및 운영적 대책 (2)

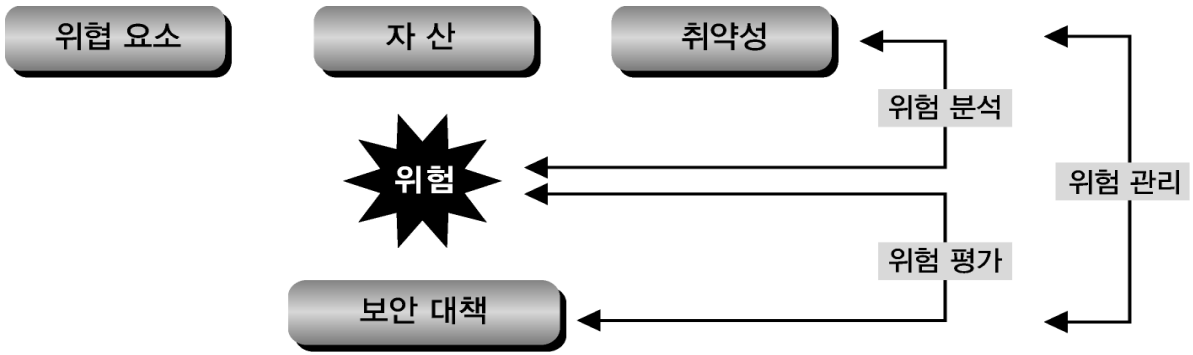
- 정보보호의 관리적 대책
  - 정보는 정보소유자의 요구에 맞는 무결성, 가용성, 비밀성을 가져야 함
  - 위험관리(Risk Management)
    - 보안관리 과정에서 가장 중요한 요소 중의 하나
    - 조직 내에 주요한 자산의 가치 및 민감도를 측정, 이에 대한 위협 및 취약성을 분석, 위험을 측정, 이를 조직에 적합한 위험수준으로 조정하기 위한 보안 대책을 선택하는 일련의 활동
    - 위험식별 -> 평가 -> 수용할 수 있는 수준으로 위험 감소화 -> 수준 유지
    - 조직이 처해 있는 위험수준을 정확히 파악하고 측정하는 위험분석 과정 필요

Risk Analysis & Management (1)

- 위험(Risk)
  - 비정상적인 일이 발생할 수 있는 가능성
    - 여러 종류의 위험 항목
      - 물리적 피해 : 화재, 물, 파괴행위, 정전, 그 밖의 자연재해
      - 사람의 실수 : 생산성을 방해하는 우연한 혹은 고의적인 행동 또는 태만
      - 장치고장 : 시스템과 주변 장비의 실패
      - 내부와 외부의 공격 : 해킹, 크래킹
      - 데이터의 남용(misuse) : 거래 비밀 공유, 사기, 정탐(espionage)과 절도
      - 데이터 손실 : 파괴적인 수단에 의한 고의적인 혹은 우연한 정보 손실
      - 응용프로그램 오류 : 전자계산 오류, 입력 오류, 버퍼 오버플로우(buffer overflow)
    - 정보시스템의 위험요소
      - 기술적 위험 : 소프트웨어 및 하드웨어 위험, 부적합한 신기술 적용
      - 조직상의 위험 : 불명확한 책임과 권한, 불합리한 업무분장
      - 절차상의 위험 : 절차와 규정의 미비, 오용, 위반, 이해부족
      - 인간에 의한 위험 : 실수, 오류, 태만, 부정, 사기, 불법접근
      - 응용시스템 위험 : 프로그램 논리적 오류, 버그, 자연재해 및 환경에 의한 위험

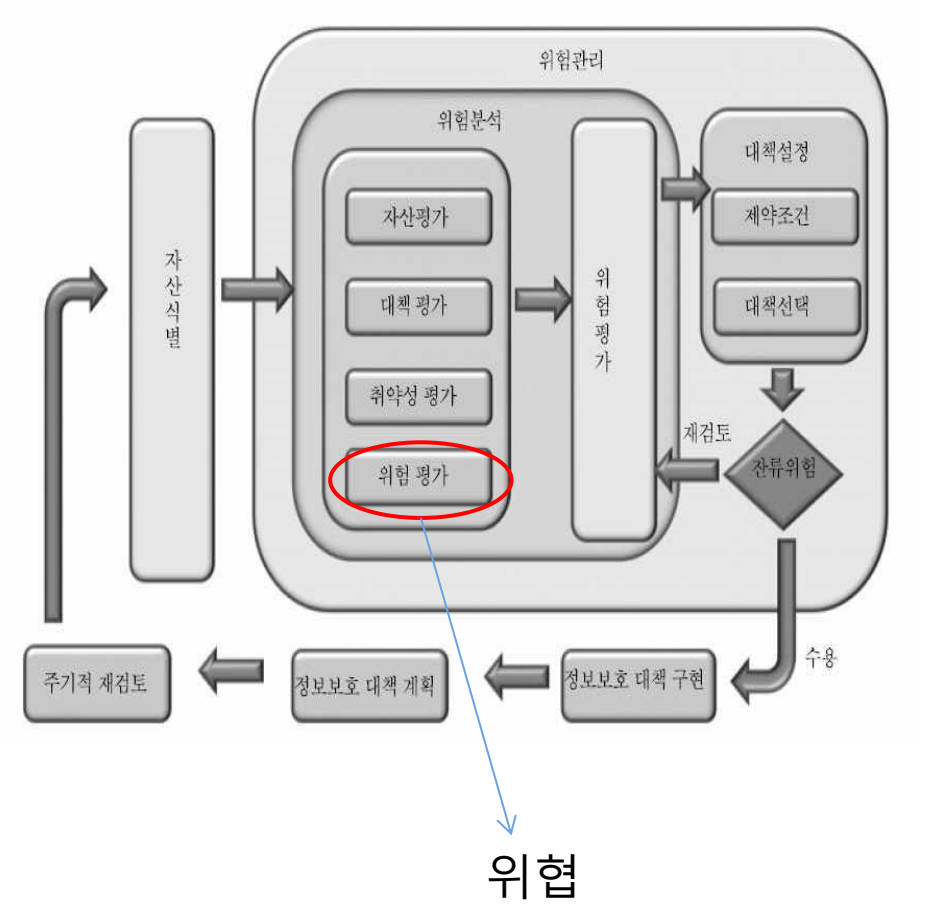
Risk Analysis & Management (2)

- 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
  - 보안대책을 수립할 때 근거를 제공
- 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 유지
  - 효과적인 보안정책 및 대책 수립을 위하여 필요한 기본적 요소



Risk Analysis & Management (3)

- 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



Risk Analysis & Management (4)

- 위험 분석
  - 위험을 식별, 발생 가능한 피해를 평가하여 보안 안전장치를 정당화하는 수단
  - 목표
    - 위험 식별
    - 잠재적 위협의 충격측정
    - 위험의 충격과 그 대책에 대한 비용간의 경제적 균형 제공
  - 위험 분석 팀
    - 조직에서의 보안 역할(Security Roles Within an Organization)
      - 최고 경영진 : 조직의 보안과 자산 보호에 대한 궁극적인 책임
      - 보안 전문가 : 보안에 대해 직무상의 책임을 가지며 최고 경영진의 명령을 수행
      - 데이터 소유자 : 조직에서 정보의 데이터 등급을 결정
      - 데이터 관리자 : 데이터의 기밀성, 무결성, 그리고 가용성을 보존하고 보호하는 방법으로 데이터를 유지
      - 사용자 : 데이터 처리 작업에 데이터를 사용
      - 감사자(auditor) : 조직에서 보안 실천과 메커니즘을 검사

Risk Analysis & Management (5)

- 위험 분석 (계속)
  - 정보자산(information assets) 분석
    - 기업이 보호하려는 정보의 가치를 모른다면, 정보를 보호하기 위해 어느 정도의 비용과 시간을 소비해야 하는지 알지 못함
    - 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

Risk Analysis & Management (6)

- 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
    - 위협분석의 수행과정
      - 발생하는 각 위험의 가능성에 관한 정보를 각 부서의 직원, 과거기록, 공식적인 보안 정보자원을 통해 수집
      - 식별된 위험 발생의 확률을 계산
      - 각 위험이 1년에 몇 번이나 발생 할 수 있는지를 나타내는 연간 예상 손실(ALE : Annualized Loss Expectancy)을 계산

Risk Analysis & Management (7)

- 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

Risk Analysis & Management (8)

- 위험 분석 (계속)
  - 취약성 분석과 대책 (계속)
    - 위협 주체, 취약성 그리고 위험의 관계

위협주체	취약성의 활용	위험의 결과
바이러스	안티바이러스 S/W 부족	바이러스 감염
해커	서버에서 실행되는 강력한 서비스	기밀한 정보에 대한 허가되지 않은 접근
사용자들	운영시스템의 잘못 설정된 매개변수	시스템 기능 불량
화재	화재감지, 소화시설 부족	시설물과 컴퓨터에 대한 피해, 인명 피해
직원	느슨한 접근제어	중요 정보 손상, 누설
계약직원	느슨한 접근제어	중요 정보 손상, 누설
공격자	서툴게 작성된 프로그램	버퍼 오버플로우 수행
침입자	보안 경계 부족	컴퓨터와 장비 도난
직원	감리(auditing) 부족	데이터 입출력에 대한 변경
공격자	엄중한 firewall 부족	서비스 거부 공격 수행

Risk Analysis & Management (9)

- 위험분석방법론
  - 정량적 방법
    - 손실 및 위험의 크기를 금액으로 나타내는 정밀한 분석이 요구되는 방법
  - 정성적 방법
    - 손실이나 위험을 개략적인 크기로 비교하는 방식
  - 혼합 접근 방법
    - 정량적 방법과 정성적 방법을 모두 이용
    - 일차적으로 정성적 방법을 이용하되 특정한 관심사는 면밀한 정량적 결정을 내리는 방식

Risk Analysis & Management (10)

- 정량적 위험 분석
  - 수학공식 접근법
    - 위협의 발생빈도를 계산하는 식을 이용하여 위험을 계산하는 방법
    - 과거자료의 획득이 어려울 경우 위협 발생 빈도를 추정하여 분석
    - 위험을 정량화하여 매우 간결하게 나타낼 수 있음
    - 기대손실을 추정하는 자료의 양이 낮다는 단점
    - 일반적인 분석절차 : 위협변수들 식별 -> 발생빈도를 추정 -> 연간손실예상(ALE : Annual Loss Expectancy)를 추정하여 계산
      - 단일 손실 예상(SLE : Single Loss Expectancy)
        - 특정한 위협이 발생했을 경우에 기업의 잠재적 손실치를 나타내는 한 사건에 할당되는 금액
        - 노출계수(Exposure Factor)
          - 인식된 위협이 특정 자산에 끼칠 수 있는 손실의 퍼센티지(%)
        - SLE = 자산가치 (asset value) X 노출계수(exposure factor)
      - 연간 발생률(ARO : Annualized Rate of Occurrence)
        - 1년 동안의 시간 단위에 발생하는 특정한 위협의 가능성을 추정하는 값
        - 범위 : 0.0(never)에서 1.0(always)까지 어떤 값도 될 수 있음
      - ALE = SLE X 연간발생률(ARO)

Risk Analysis & Management (11)

- 정량적 위험 분석 (계속)
  - 확률 분포법
    - 미지의 사건을 추정하는데 사용되는 방법
    - 미지의 사건을 확률적(통계적) 편차를 이용하여 최저, 보통, 최고의 위험평가를 예측
    - 확률적으로 추정하는 방법이기 때문에 정확성이 낮음
    - 일반적인 분석 절차 : 최고와 최저를 제외한 추정치의 산술 평균치를 구함 → 추정 산술 평균치에 표준화된 인자 값을 곱함 → 기대 위험 확률치를 구함
    - 정량적 접근 시도
      - 위협과 위험의 가능성을 결정할 때 구체적인 확률 퍼센티지(percentages)를 제공
    - 분석의 각 요소
      - 자산 가치(asset value), 위협 빈도(threat frequency), 취약성의 심각성(severity of vulnerability), 피해 영향(impact damage), 안전장치 비용(safeguard costs), 안전장치 효과성(safeguard effectiveness), 불확실성(uncertainty), 확률(개연성) 항목(probability items)가 수량화 되고 잉여 위험을 결정하기 위해 방정식에 입력 됨

Risk Analysis & Management (12)

- 정성적 위험 분석
  - 다양한 위험 가능성의 시나리오에 정성적 방법을 투영시키고 위협의 심각성과 자산의 중요성에 순위를 정함
  - 정성적 분석 기술
    - 판단, 직관, 경험을 포함
  - 정성적 기법의 예
    - 델파이(Delphi)
    - 브레인스토밍(brainstorming)
    - 스토리보딩(storyboarding)
    - 포커스그룹(focus group)
    - 설문(surveys)
    - 질문지(questionnaires),
    - 점검표(checklists)
    - 일대일 모임(one on one meeting)
    - 면접(interviews)

Risk Analysis & Management (13)

- 정성적 위험 분석 (계속)
  - 델파이법
    - 시스템에 관한 전문적인 지식을 가진 전문가의 집단을 구성하고 위험을 분석 및 평가하여 정보시스템이 직면한 다양한 위협과 취약성을 토론을 통해 분석하는 방법
    - 위험분석을 짧은 시간에 도출할 수 있어 시간과 비용을 절약
    - 전문가의 지식과 토론만으로 위협 요소 등을 추정하기 때문에 추정의 정확도가 낮음
    - 일반적인 분석 절차
      - 전문가 팀은 위험의 순위를 나열해서 위협을 식별
      - 팀 구성원 각자의 견해를 종합하여 일치된 결론을 찾음
      - 일치된 결론을 토대로 위험순위를 나열하여 위협과 취약성의 수준을 결정

Risk Analysis & Management (14)

- 정성적 위험 분석 (계속)
  - 시나리오법
    - 어떤 사건도 기대대로 발생하지 않는다는 사실에 근거하여 일정 조건하에서 위협에 대한 발생 가능한 결과들을 추정하는 방법
    - 장점 : 적은 정보를 가지고 전반적인 가능성을 추론할 수 있고, 위험분석 팀과 관리 층간의 원활한 의사소통을 가능케 함
    - 단점 : 발생 가능한 사건의 이론적인 추측에 불과하고 정확성, 완성도, 이용기술의 수준 등이 낮음
    - 일반적인 분석 절차
      - 위협이 발생 할 수 있는 분야의 전문가로 팀을 구성
      - 위험 가능성이 있는 상황, 활률 요인, 비용추정 중에서 바람직한 결과 하나만을 산출
      - 가능성 있는 위협으로 인해서 발생될 수 있는 상황을 이야기 식으로 기술

Risk Analysis & Management (15)

- 정성적 위험 분석 (계속)
  - 순위 결정법
    - 비교 우선 순위결정표에 위험 항목들의 서술적 순위를 결정하는 방법
    - 장점 : 위험분석에 소요되는 시간과 분석하여야 하는 자원의 양이 적음
    - 단점 : 위험 추정의 정확도가 낮음
    - 일반적인 분석 절차
      - 위협요인에 대한 상호비교를 통해 우선순위를 결정
      - 두 가지 위협만을 비교하면서 의견 차이를 서로 토론하여 조정
      - 두 가지 위협에 대해서 팀원들이 제시한 값을 합산하고, 제시된 값들을 각 위협별로 합산
      - 합산한 값을 근거로 위협의 우선순위를 결정

Risk Analysis & Management (16)

- 정량적 분석과 정성적 분석의 비교
  - 정량적 분석과 정성적 분석의 목표
    - 기업의 실제 위험을 평가
    - 위험의 심각성을 분류함
    - 실제적인 예산을 사용하여 대책 마련
  - 정량적, 정성적 분석의 특징

특성	정량적분석	정성적 분석
복잡한 계산 요구	O	
추측(guess) 작업이 연관되는 정도		O
쉽게 자동화 되는가	O	
비용/이익 분석 제공	O	
독립적이고 객관적인 측정 기준 이용	O	
해당 과정을 잘 아는 스텝의 의견 제공		O
1년의 기간 동안에 발생할 수 있는 피해 도출	O	

Risk Analysis & Management (17)

- 총체적 위험과 잔류 위험(Total Risk versus Residual Risk)
  - 총체적 위험 : 기업이 어떠한 안전장치도 설치하지 않았을 경우의 위험
    - 위협 X 취약성 X 자산가치 = 총체적 위험
  - 잔류 위험 : 보안대책과 이에 따른 안전장치가 설치된 후에도 남아 있는 위험
    - (위협 X 취약성 X 자산가치) X 제어결함 = 잔류 위험