

정 보 보 안 기 사 스 터 디

스터디 4주차

발 표 자 이 승 현

목차

01 위험 관리 및 분석

초련 (初戀) (First Love) (Tech

3주차 - Google 드라이브

기술문제

위험관리 및 분석 :: Gamja's Farm

iLiFO 지킴 :: 관지덤 프로젝트 위험관

cms2580.cafe24.com/v2/production/select2.jsp

CMS

MENU

Home

기술문제

Book

시험일정

IT 기술사 문제출제

동영상 강좌

정보보안기사 실기

9 회

전체 보기

8. 시스템에 관한 전문적인 지식을 가진 전문가의 집단을 구성하고, 정보시스템이 직면한 다양한 위협과 취약성을 토론을 통해 분석하는 방법

해설

위르

9. 정보보호시스템 공통평가기준에 있는 내용이다.
"A"이라 함은 평가대상 범주를 위한 특정 소비자의 요구에 부합하는 구현에 독립적인 보안요구사항의 집합을 말한다.
"B"라 함은 식별된 평가대상의 평가를 위한 근거로 사용되는 보안요구사항과 구현 명세의 집합을 말한다.
"C"이라 함은 공통평가기준에서 미리 정의된 보증수준을 가지는 보증 컴포넌트로 이루어진 패키지를 말한다.

해설

10. 위협은 비정상적인 일이 발생할 수 있는 가능성을 말하며, 위협분석은 위협을 분석하고 해석하는 과정이다. 위협을 구성하는 4가지 기본요소를 쓰시오.

해설

서술형

11. 전자서명법에 따라 공인인증기관이 발급한 공인인증서의 효력이 소멸하는 4가지 사유를 쓰시오

해설

cms2580@naver.com

8. 시스템에 관한 전문적인 지식을 가진 전문가의 판단을 구성하고, 정보시스템의 위험한 다양한 위험과 취약성을 도출을 통해 분석하는 방법

해설

9. 정보보호시스템 공통평가기준에 있는 "A"이라 함은 평가대상 범주를 위한 특정 "B"라 함은 식별된 평가대상의 평가를 위한 "C"이라 함은 공통평가기준에서 미리 정의

해설

10. 위험은 비정상적인 일이 발생할 수 있는 가능성을 말하며, 위험분석은 위험을 분석하고 해석하는 과정이다. 위험을 구성하는 4가지 기본요소를 쓰시오.

해설

서술형

11. 전자서명법에 따라 공인인증기관이 발급한 공인인증서의 효력이 소멸하는 4가지 사유를 쓰시오

해설

cms2580@naver.com

8282 - YouTube Music

3주차 - Google 드라이브

기술문제

위험관리 및 분석 :: Gamja's Farm

iLiFO 지점 :: 관지점 프로젝트 위험관

주의 요함 | cms2580.cafe24.com/v2/production/select2.jsp

CMS

MENU

Home

기술문제

Book

시험일정

IT 기술사 문제출제

동영상 강좌

정보보안기사 실기

9 회

전체 보기

8. 시스템에 관한 전문적인 지식을 가진 전문가의 판단을 구성하고, 정보시스템의 위험한 다양한 위험과 취약성을 도출을 통해 분석한 방법

해설

자산, 취약성, 위협, 정보보호대책

Close

위르

9. 정보보호시스템 공통평가기준에 있는

"A"이라 함은 평가대상 범주를 위한 특정

"B"라 함은 식별된 평가대상의 평가를 위

"C"이라 함은 공통평가기준에서 미리 정의

해설

10. 위험은 비정상적인 일이 발생할 수 있는 가능성을 말하며, 위험분석은 위험을 분석하고 해석하는 과정이다. 위험을 구성하는 4가지 기본요소를 쓰시오.

해설

서술형

11. 전자서명법에 따라 공인인증기관이 발급한 공인인증서의 효력이 소멸하는 4가지 사유를 쓰시오

해설

cms2580@naver.com

프로젝트 위험관리

개념 프로젝트 위험(Risk)의 개념 - 프로젝트 전체 기간 중 발생하여 프로젝트의 정상적인 납기, 품질, 원가에 영향을 줄 수 있는 사건으로써, 프로젝트 수행 중에 반드시 식별되고 관리/해결해야 할 프로젝트 관리요소 - 총 위험 = 위험 x 취약성 x 자산 가치 위험관리(Risk Management)의 정의 - 위험을 식별하고 분석하여 대응하는 과정 - 기회는 극대화하고 위험은 최소화하여 프로젝트의 성공 가능성을 높이는 일련의 활동

I. Risk의 정성적, 정량적 분석을 통한 관리기법, 프로젝트 위험관리의 개요

가. 프로젝트 위험(Risk)의 개념

- 프로젝트 전체 기간 중 발생하여 프로젝트의 정상적인 납기, 품질, 원가에 영향을 줄 수 있는 사건으로써, 프로젝트 수행 중에 반드시 식별되고 관리/해결해야 할 프로젝트 관리요소
- 총 위험 = 위험 x 취약성 x 자산 가치

나. 위험관리(Risk Management)의 정의

- 위험을 식별하고 분석하여 대응하는 과정
- 기회는 극대화하고 위험은 최소화하여 프로젝트의 성공 가능성을 높이는 일련의 활동

다. 위험관리의 목적

- 프로젝트의 정상적인 수행을 보장
- 위험요소의 관리/제거를 통하여 성공적 프로젝트 수행의 기반구축
- 위험을 예상하고 대응함으로써 프로젝트 성공 가능성을 높임

위험 관리 및 분석

정보보호 체계에서 위험관리는 위험을 식별, 분석, 평가, 보호대책을 수립 하는 일련의 활동.

정의: 조직의 자산을 식별하고 위험을 평가하며 조직의 재해, 장애 등 손실을 최소화하기 위한 절차 혹은 연속적인 행위이다.

위험관리 구성

1. 자산 : 조직에 가치가 있는 자원들
2. 위협 : 위협과 취약점을 이용하여 조직의 자산에 손실, 피해를 가져올 가능성
3. 위협 : 조직, 기업의 자산에 악영향을 끼칠 수 있는 조건, 사건, 행위
4. 취약점 : 위협이 발생하기 위한 조건 및 상황

위험분석 : 보호 대상, 위협 요소, 취약성 등에 대한 자료 수집 및 분석

위험평가 : 분석 결과를 기초로 하여 보안 현황을 평가하고 적절한 방법을 선택하여 효과적으로 위험 수준을 낮추기 위한 과정

위험관리 활동

1. 위험성향 : 수용할 준비가 된 위협의 총량을 의미하며, 영향의 크기와 발생빈도로 정의됨
2. 위험허용범위 : 위험성향에 근거한 위험수준으로부터 수용가능한 최대편차
3. 위험대응 : 식별된 위협의 발생 가능성과 영향에 대한 대응조치

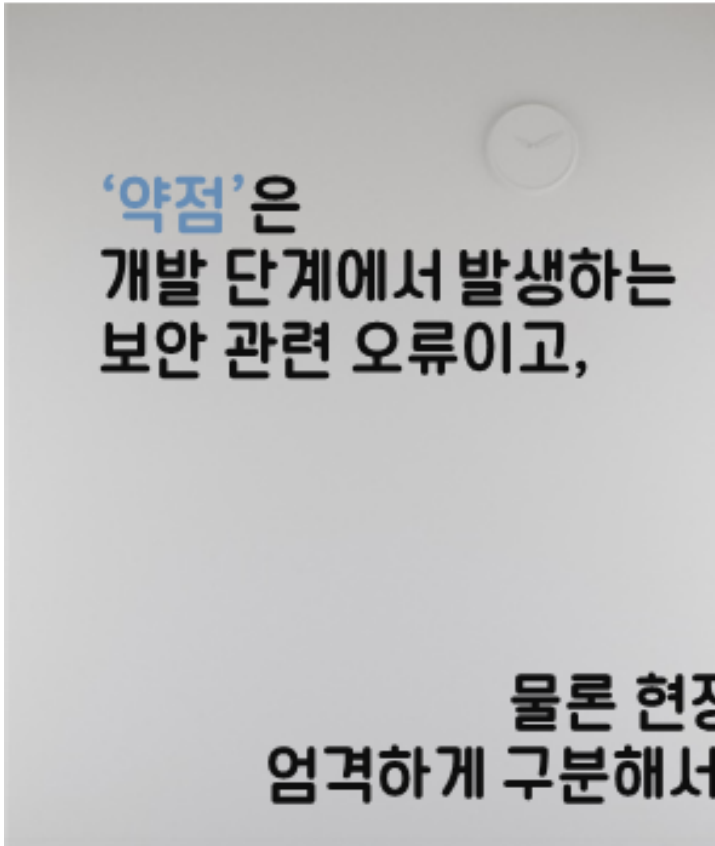
약점? 취약점? 위협? 위험?
정리가 필요해!



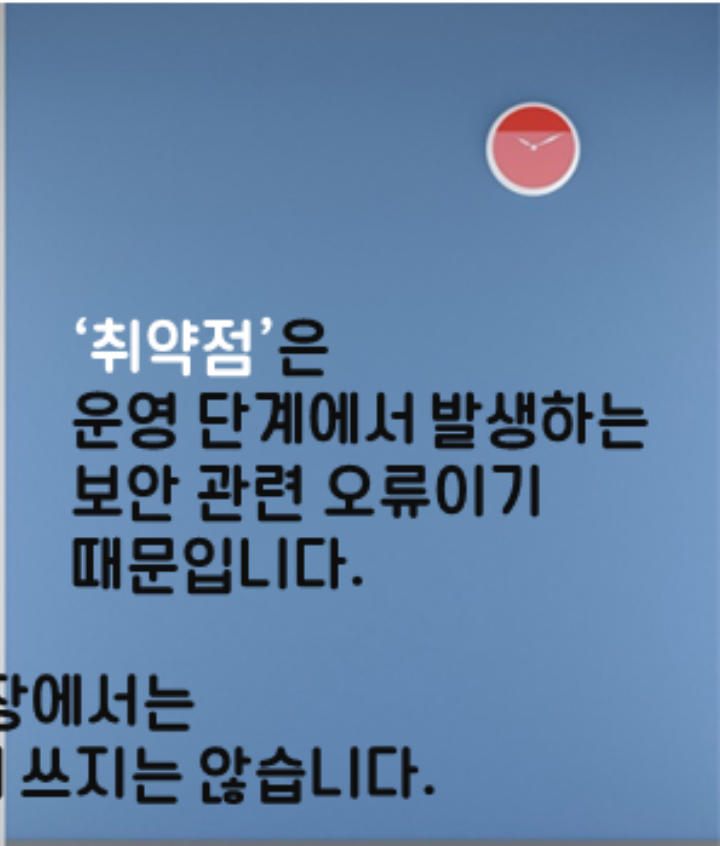
새로운 악성코드가 발견되면
대개 어떠한 약점을 이용하여
만들어졌는지가 함께 발표됩니다.

예를 들면 이번
'워너크라이(WannaCry) 랜섬웨어'는
Windows의 SMBv2 취약점을 악용해
만들어졌다'는 것처럼요.

사실 보안 전문가 여러분에게는
‘약점’보다는 **‘취약점’**이란 말이 더 익숙하시겠지만,
이 둘은 사전적으로 **다른 의미**입니다.



‘약점’은
개발 단계에서 발생하는
보안 관련 오류이고,



‘취약점’은
운영 단계에서 발생하는
보안 관련 오류이기
때문입니다.

물론 현장에서는
엄격하게 구분해서 쓰지는 않습니다.



한 보안 전문가는

“보안 **약점**은 weakness로
‘공격에 활용될 여지가 있는 오류’
즉, 이론상 존재하는 위험 요소를 말하고,

보안 **취약점**은 vulnerability로
‘실제로 공격 구현이 가능한 오류’
즉, 구현이 실제적으로 가능한 것”이라고

설명했습니다.

‘위협(threat)’과
‘위험(risk)’은 어떨까요?

‘위협’은
위험을 일으킬 소지가 다분한 요소를 말하며,

‘위험’은
위협 요소가 일으킬 수 있는 피해를 말합니다.

또 다른 보안 전문가는 이렇게 설명했습니다.

“위협은 보통 **제어가 되지 않는**다는 게
가장 큰 특징입니다.

위험은 줄일 수 있습니다.
즉, **관리가 가능**하다는 겁니다.

취약점(약점)은 조치가 가능합니다.
취약점이 무엇인지 찾아내고
그걸 없애는 게 중요하다는 것이죠.”





이렇게 기본 개념을 구분하는 것이 중요한 건
이제 남녀노소 모두가 보안에 참여해야 하는 때이고
서로가 같은 말을 사용하고 이해해야
‘보안 전략’이 최대의 효과를 발휘할 수 있기 때문입니다.

기본 개념이 톱니바퀴처럼 튼튼히 맞물려야
더욱 안전할 수 있겠죠?

01

위험관리 활동

1. 위험성향 : 수용할 준비가 된 위험의 총량을 의미하며, 영향의 크기와 발생빈도로 정의됨
2. 위험허용범위 : 위험성향에 근거한 위험수준으로부터 수용가능한 최대편차
3. 위험대응 : 식별된 위험의 발생 가능성과 영향에 대한 대응조치

위험분석

- 접근방법에 따른 위험분석기법

1. 기준선 접근법 (베이스라인 접근법) : 모든 시스템에 대하여 보호의 기준 수준을 정하고 이를 달성하기 위해 일련의 보호대책을 선택, 시간 및 비용이 적고 모든 조직에서 기본적으로 필요한 보호 대책 선택이 가능, 조직의 특성 고려의 부족으로 부서별로 적정 보안수준보다 높거나 낮게 보안통제 적용
2. 전문가 판단 (비정형 접근법) : 정형화된 방법을 사용하지 않고 전문가의 지식과 경험에 따라서 위험을 분석, 비용적인 면에서 작은 조직에 효과적이지만 구조화된 접근방법이 없으므로 위험을 제대로 평가하기 어렵고 보호 대책의 선택 및 소요비용을 합리적으로 도출하기 힘들. 계속적으로 반복되는 보안관리 및 보안감시, 사후관리로 제한됨.
3. 상세위험분석 : 자신의 가치를 측정하고 자산에 대한 위험 정도와 취약점을 분석하여 위험 정도를 결정, 조직 내에 적절한 보안 수준 마련 기대, 전문적 지식과 노력이 많이 소요됨, 정성적 분석기법과 정량적 분석기법이 존재함.
4. 복합적 접근법 : 먼저 조직 활동에 대한 필수적이고 위험이 높은 시스템을 식별하고 이러한 시스템은 상세 위험 분석 기법으로 적용, 그렇지 않은 부분은 기준선 접근법으로 적용, 빠르게 보안 전략 구축 및 시간과 노력을 효율적으로 사용 가능, 고위험 영역이 잘못 식별 될 경우 위험분석비용이 낭비되거나 부적절하게 사용

01

정량적 위험분석과 정성적 위험분석

ALE : 연간 기대 손실, 손실 크기, 정량적인 위험분석의 대표적인 방법으로 특정 자산에 대하여 실현된 위협의 모든 경우에 대해서 가능한 연간 비용

SLE : 위험 발생 확률, 특정 위협이 발행하여 예상되는 1회 손실액($SLE = 자산가치 * EF(1회 손실액)$)

ARO : 매년 특정한 위협이 발생할 가능성에 대한 빈도수, 혹은 특정 위협이 1년에 발생할 예상 빈도수

정량적 위험분석 : 비용/가치 분석, 예산 계획, 자료 분석이 용이, 분석 시간, 노력, 비용이 크고 정확한 정량화 수치를 얻기 어려움.

-> 수학기초 접근법, 확률 분포 추정법, 확률 지배, 몬테카를로 시뮬레이션, 과거 자료 분석법

정성적 위험분석 : 손실 크기를 화폐가치로 표현하기 어려움, 위험크기는 기술변수로 표현, 분석시간이 짧고 이해가 쉬움, 금액화 하기 어려운 정보의 평가 기능, 평가 결과 주관적임, 비용효과 분석이 쉽지않음

-> 델파이법, 시나리오법, 순위 결정법, 질문서법

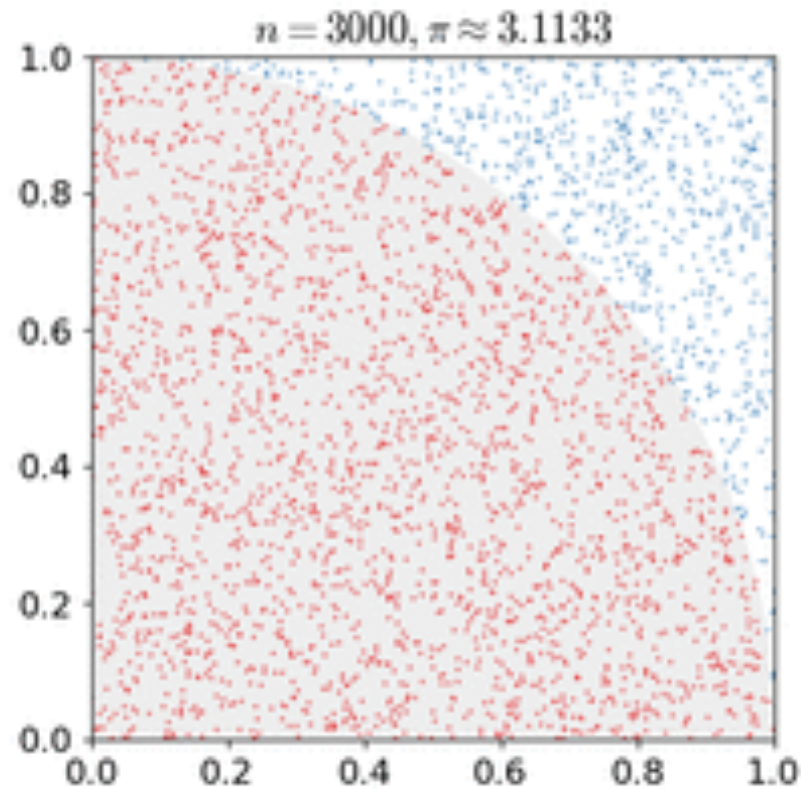
확률분포법 : 미지의 사건을 추정하는데 사용되는 방법, 이 방법은 미지의 사건을 확률적(통계적) 편차를 이용하여 최저, 보통, 최고의 위험평가를 예측할 수 있다. 그러나 확률적으로 추정하는 방법이기 때문에 정확성이 낮다.

시나리오법 : 어떤 사건도 기대대로 발생하지 않는다는 사실을 근거하여 일정 조건하에서 위협에 대한 발생 가능한 결과들을 추정하는 방법, 이 방법은 적은 정보를 가지고 전반적인 가능성을 추론할 수 있고, 위험분석팀과 관리층 간의 원활한 의사소통을 가능하게 한다. 그러나 발생 가능한 사건의 이론적인 추측에 불과하고 정확도, 완성도, 이용기술의 수준 등이 낮다

델파이법 : 시스템에 관한 전문적인 지식을 가진 전문가의 집단을 구성하고, 정보시스템이 직면한 다양한 위협과 취약성을 토론을 통해 분석하는 방법이다

01

“ 몬테카를로 시뮬레이션 ”



https://www.iitp.kr/resources/file/2019ICT_1_v2.pdf

THANK
YOU

발 표 자 이 승 현