제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️ ppt: 💾

참고 ppt : https://drive.google.com/open?id=1DtJiO0sWjxHARL3ZKNfQndWlykR8IXUZ

😃 보안성 공학(Security Engineering)

😎 보안성과 확실성(📘 388p.)

📌💾 ppt 참고내용

❓ **컴퓨터 보안과 보안성 공학과의 관계를 말해 보시오.**

- 컴퓨터보안의 서브 필드이다

❓ **보안성 공학이란 무엇인지를 말해 보시오.**

- 악의적인 공격으로 부터 견뎌내도록 시스템을 개발하고 유지보수할 때 필요한 도구와 기법을 담은 학문

📌보안의 세가지 관점인 기밀성 무결성 가용성을 말해보시오
(📣교수님 | 시험에 자주나온다)

- **기밀성(Confidentiality) 김일성**
  - 허가받지도 않은 사람이 시스템이 있는 내 정보를 접근하거나 들여다 보는 것
- **무결성(Integrity)**
  - 내정보가 데미지를 입어서 신뢰할 수 없는 정보가 될 수 있다.
  - 정보가 데미지를 입었거나 손상되어 믿을 수 없는 상태
- **가용성 (Availability)**
  - 더이상 시스템을 사용하지 못하도록 하는 것
    EX) dos 공격

❓ 세단계 수준인 **기반 구조보안, 애플리캐이션보안, 운영보안**을 말해보시오

- **기반구조 보안**
  - 이거보완점 관리하는
  - 📘 기반구조와 공유 서비스 집합을 조직에 제공하는 모든 시스템 및 네트워크의 보안성 유지와 관련된다.
- **애플리케이션 보안**
  - 각각의 개별 시스템들의 보안과 관련된 것
  - 📘 개별 애플리케이션 시스템 또는 관련 있는 시스템들의 그룹의 보안성과 관련된다.
- **운영보안**

제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾

    - 보안정책이나 접근제어나 그런것들을 사람들이 해주는 안전한 운영과 이용에 관련된 운영보안
- 📘 조직 시스템의 보안성 있는 운영 및 사용과 관련된다.

❓ **애플리케이션 보안에 대해 말해보시오**

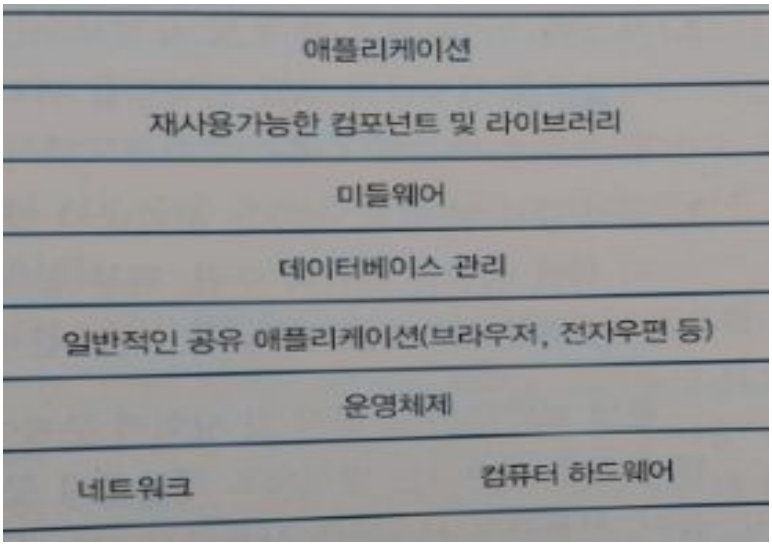
- 시스템이 공격에 의해 버티도록 설계된 구조

❓ **기반구조 보안에 대해 말하시오**

- 공격에 저항할 수 있게 설정해주는 시스템
  EX) 사용자의 권한문제, 소프트웨어를 유지보수, 공격을 모니터링 하고 감지하고 공격을 받았다면 복구(회복)하는것

❓ **운영 보안에 대해 말해보시오**

- 사람과 사회적 이슈와 관련이 깊다
- 시스템의 보안이 너무 강하면 사용하는데 불편함이 있어 타협점을 잘 찾는 것이 좋다.
-



보안을 고려해야 하는 시스템 계층

📖 책 참고내용

제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾

😎 보안과 신뢰성(📘 390p.)

📌💾 ppt 참고내용

보안의 정의

- 시스템이 자신을 외부의 공격으로 부터 방어하는 능력
- 📘 보안성은 악의적인 내외부의 공격으로부터 자신을 방어하는 시스템의 능력을 나타내는 시스템 특성이다.

보안의 중요성

- 많은 시스템이 서로 연관되어 있기 때문에 외부로부터의 접근이 인터넷을 통해 가능해지기 때문에

보안이 왜 가용성, 신뢰성, 안정성의 필수 선행조건인지 말해보시오

-

보안용어 📘391p.

그림 13.2 보안 용어

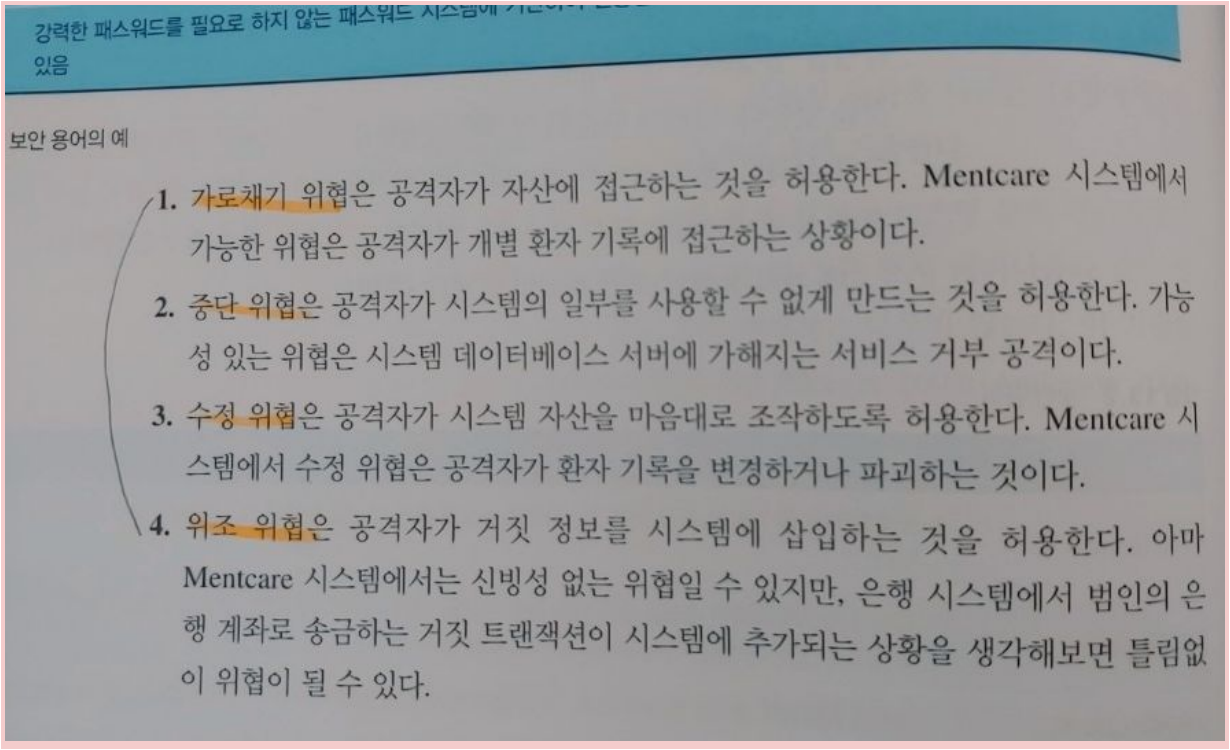
용어	정의
자산(asset)	보호되어야 할 가치를 가진 어떤 것. 자산은 소프트웨어 시스템 자체나 그 시스템에 의해 사용되는 데이터가 될 수 있다.
공격(attack)	시스템 자산에 어떠한 손실을 일으키는 것을 목표를 하는 시스템 취약점의 부당한 이용. 공격은 시스템의 외부(외부 공격) 또는 권한이 있는 내부자(내부 공격)로부터 올 수 있다.
통제(control)	시스템 취약점을 줄이는 방어적 조치. 약한 접근 통제 시스템의 취약점을 줄이는 통제의 한 예가 암호화이다.
노출(exposure)	컴퓨터 시스템의 가능한 손실이나 손해. 이것은 데이터에 대한 손실 혹은 손상이 될 수 있고 보안 침입 후에 복구가 필요하면 시간과 노력의 손실이 될 수 있다.
위협(threat)	손실 혹은 손해를 초래할 가능성이 있는 상황. 공격받기 쉬운 시스템 취약점을 위협으로 생각할 수 있다.
취약점(vulnerability)	손실이나 손해를 초래하기 위해 이용될 수 있는 컴퓨터 기반 시스템의 약점이다.

Control (통제 X --> 보호조치 대책)

📘 **392p.**

제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾

📌 보안 위협의 네 유형을 말해 보시오.(📣**교수님 | 시험에 나왔다)**

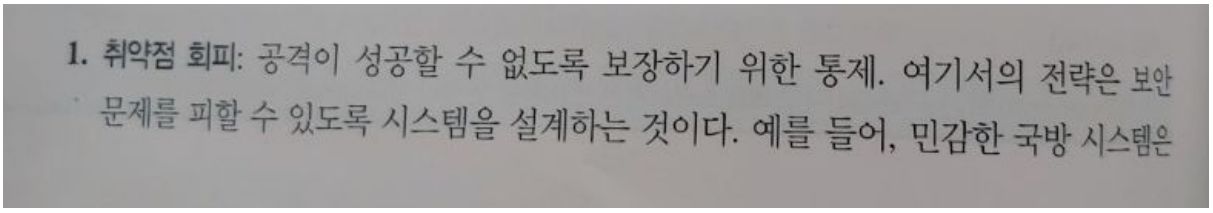


강력한 패스워드를 필요로 하지 않는 패스워드 시스템에 [illegible]
있음

보안 용어의 예

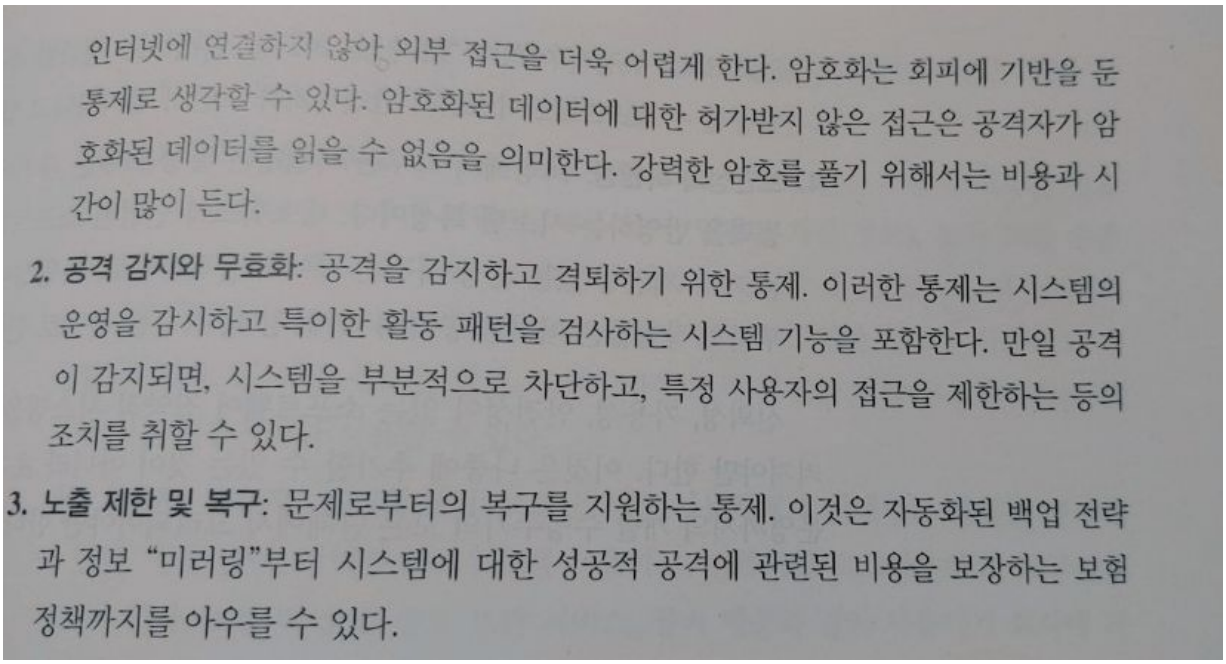
1. 가로채기 위협은 공격자가 자산에 접근하는 것을 허용한다. Mentcare 시스템에서 가능한 위협은 공격자가 개별 환자 기록에 접근하는 상황이다.
2. 중단 위협은 공격자가 시스템의 일부를 사용할 수 없게 만드는 것을 허용한다. 가능성 있는 위협은 시스템 데이터베이스 서버에 가해지는 서비스 거부 공격이다.
3. 수정 위협은 공격자가 시스템 자산을 마음대로 조작하도록 허용한다. Mentcare 시스템에서 수정 위협은 공격자가 환자 기록을 변경하거나 파괴하는 것이다.
4. 위조 위협은 공격자가 거짓 정보를 시스템에 삽입하는 것을 허용한다. 아마 Mentcare 시스템에서는 신빙성 없는 위협일 수 있지만, 은행 시스템에서 범인의 은행 계좌로 송금하는 거짓 트랜잭션이 시스템에 추가되는 상황을 생각해보면 틀림없이 위협이 될 수 있다.

세 가지 보안성 보증 전략을 말해 보시오.(책392)



1. **취약점 회피**: 공격이 성공할 수 없도록 보장하기 위한 통제. 여기서의 전략은 보안 문제를 피할 수 있도록 시스템을 설계하는 것이다. 예를 들어, 민감한 국방 시스템은

제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾



인터넷에 연결하지 않아 외부 접근을 더욱 어렵게 한다. 암호화는 회피에 기반을 둔 통제로 생각할 수 있다. 암호화된 데이터에 대한 허가받지 않은 접근은 공격자가 암호화된 데이터를 읽을 수 없음을 의미한다. 강력한 암호를 풀기 위해서는 비용과 시간이 많이 든다.

2. **공격 감지와 무효화**: 공격을 감지하고 격퇴하기 위한 통제. 이러한 통제는 시스템의 운영을 감시하고 특이한 활동 패턴을 검사하는 시스템 기능을 포함한다. 만일 공격이 감지되면, 시스템을 부분적으로 차단하고, 특정 사용자의 접근을 제한하는 등의 조치를 취할 수 있다.

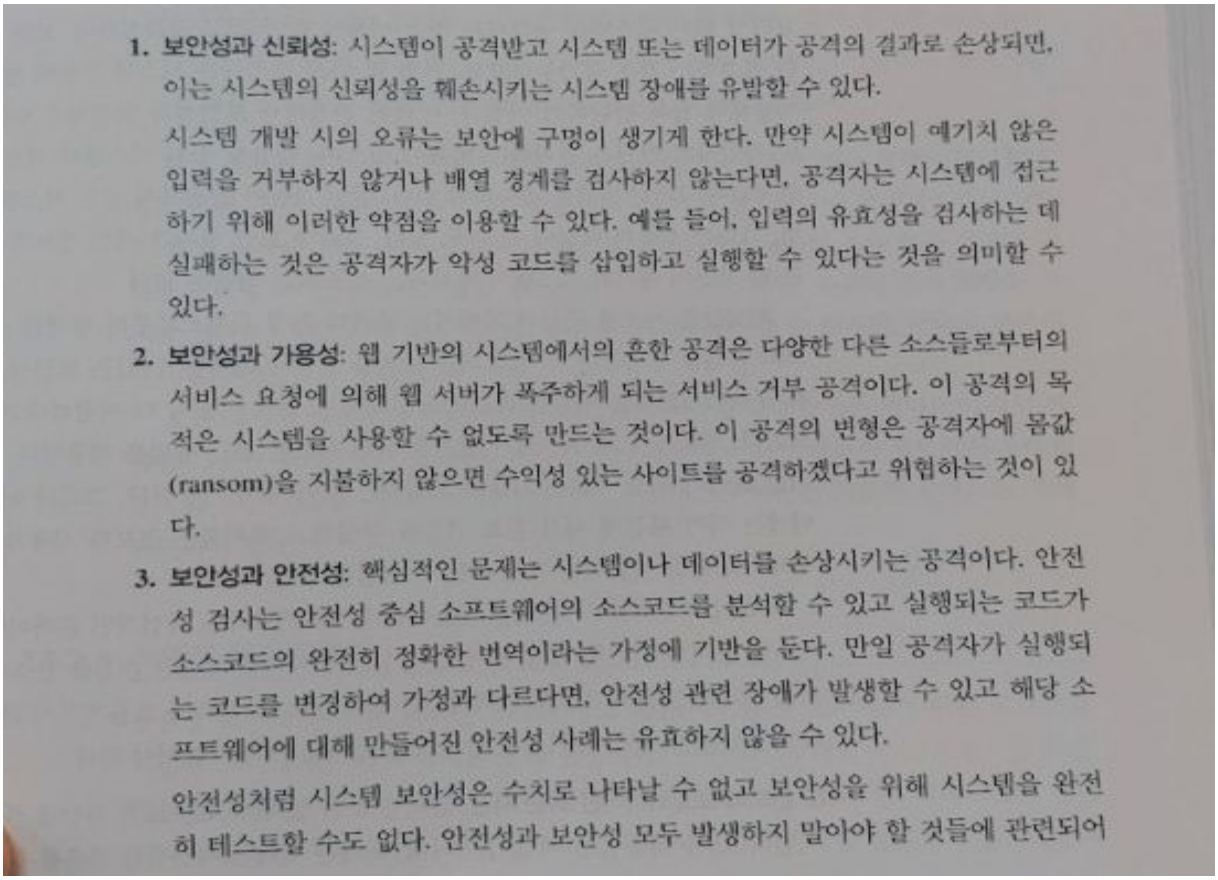
3. **노출 제한 및 복구**: 문제로부터의 복구를 지원하는 통제. 이것은 자동화된 백업 전략과 정보 "미러링"부터 시스템에 대한 성공적 공격에 관련된 비용을 보장하는 보험 정책까지를 아우를 수 있다.

보안안전

<table>
<tr><td colspan="2">Prevention(예방)</td><td rowspan="2">사
고</td><td>mitigation(완화)</td></tr>
<tr><td>Avoidance
(회피)</td><td>Detection &
Elimination
(감지 및 제거)</td><td>Limitation & recovery
(제한 및 복구)</td></tr>
</table>

보안성과 확실성의 다른 속성과의 관계를 말해 보시오.

제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾



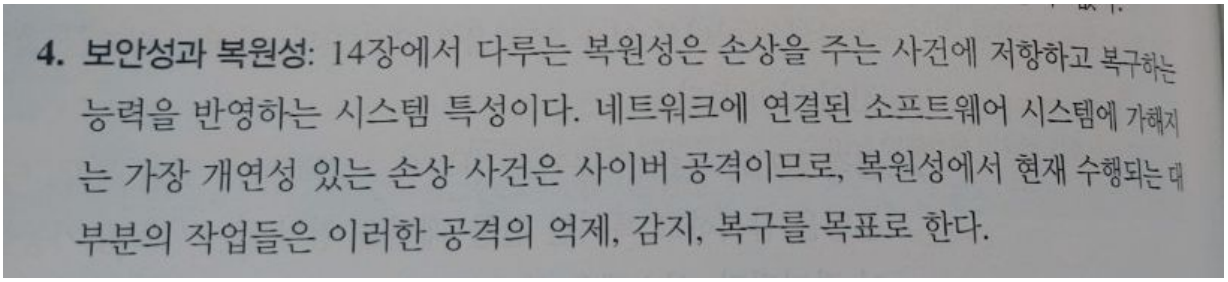
1. **보안성과 신뢰성**: 시스템이 공격받고 시스템 또는 데이터가 공격의 결과로 손상되면, 이는 시스템의 신뢰성을 훼손시키는 시스템 장애를 유발할 수 있다.

   시스템 개발 시의 오류는 보안에 구멍이 생기게 한다. 만약 시스템이 예기치 않은 입력을 거부하지 않거나 배열 경계를 검사하지 않는다면, 공격자는 시스템에 접근하기 위해 이러한 약점을 이용할 수 있다. 예를 들어, 입력의 유효성을 검사하는 데 실패하는 것은 공격자가 악성 코드를 삽입하고 실행할 수 있다는 것을 의미할 수 있다.

2. **보안성과 가용성**: 웹 기반의 시스템에서의 흔한 공격은 다양한 다른 소스들로부터의 서비스 요청에 의해 웹 서버가 폭주하게 되는 서비스 거부 공격이다. 이 공격의 목적은 시스템을 사용할 수 없도록 만드는 것이다. 이 공격의 변형은 공격자에 몸값(ransom)을 지불하지 않으면 수익성 있는 사이트를 공격하겠다고 위협하는 것이 있다.

3. **보안성과 안전성**: 핵심적인 문제는 시스템이나 데이터를 손상시키는 공격이다. 안전성 검사는 안전성 중심 소프트웨어의 소스코드를 분석할 수 있고 실행되는 코드가 소스코드의 완전히 정확한 번역이라는 가정에 기반을 둔다. 만일 공격자가 실행되는 코드를 변경하여 가정과 다르다면, 안전성 관련 장애가 발생할 수 있고 해당 소프트웨어에 대해 만들어진 안전성 사례는 유효하지 않을 수 있다.

   안전성처럼 시스템 보안성은 수치로 나타날 수 없고 보안성을 위해 시스템을 완전히 테스트할 수도 없다. 안전성과 보안성 모두 발생하지 말아야 할 것들에 관련되어



4. **보안성과 복원성**: 14장에서 다루는 복원성은 손상을 주는 사건에 저항하고 복구하는 능력을 반영하는 시스템 특성이다. 네트워크에 연결된 소프트웨어 시스템에 가해지는 가장 개연성 있는 손상 사건은 사이버 공격이므로, 복원성에서 현재 수행되는 대부분의 작업들은 이러한 공격의 억제, 감지, 복구를 목표로 한다.

📖 책 참고내용

제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾

😎 보안성과 조직(📘 394p.)

📌💾 ppt 참고내용

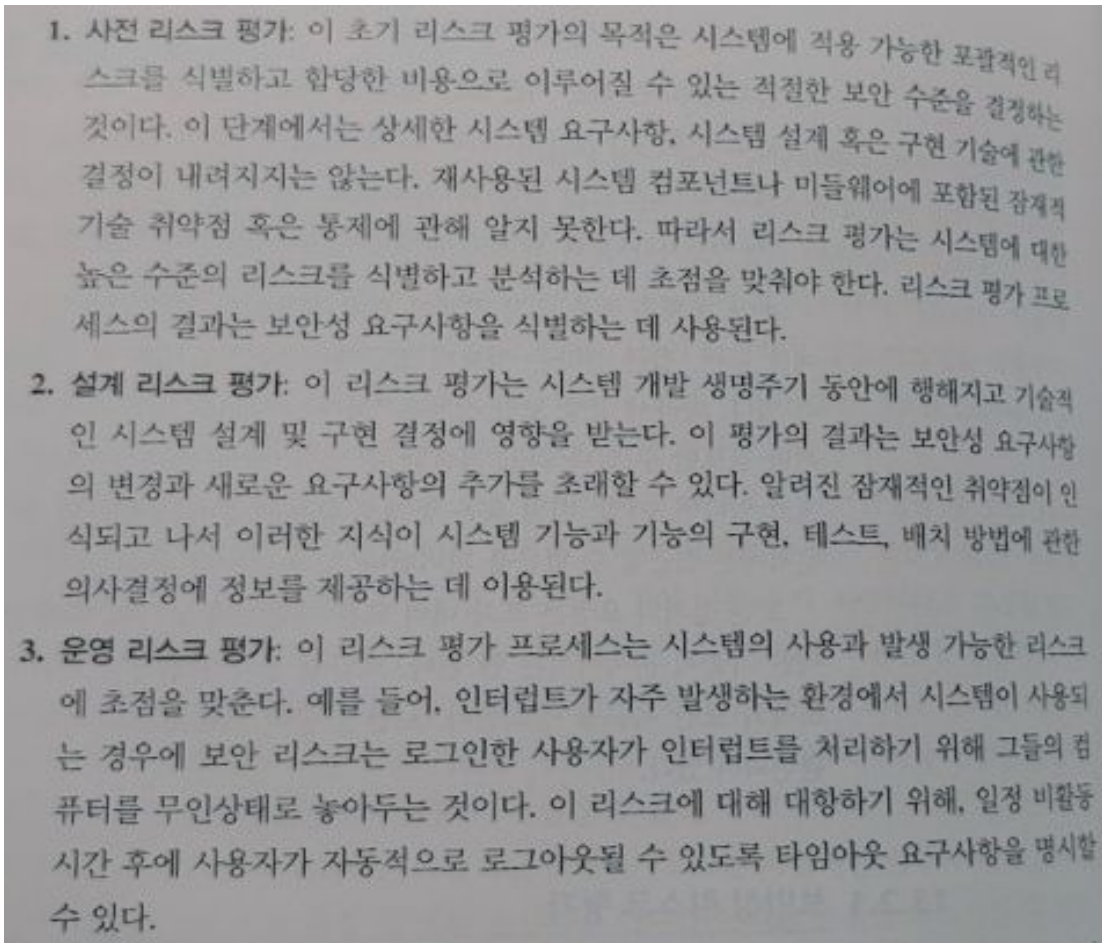
보안성을 갖추려면 왜 비용이 많이 소요되는지

-

왜 자산 가치 이상의 비용으로 자산을 보호할 필요가 없는지 .

-

보안 의사 결정을 지원하기 위해서 사용되는 리스크-기반 방법



1. 사전 리스크 평가: 이 초기 리스크 평가의 목적은 시스템에 적용 가능한 포괄적인 리스크를 식별하고 합당한 비용으로 이루어질 수 있는 적절한 보안 수준을 결정하는 것이다. 이 단계에서는 상세한 시스템 요구사항, 시스템 설계 혹은 구현 기술에 관한 결정이 내려지지는 않는다. 재사용된 시스템 컴포넌트나 미들웨어에 포함된 잠재적 기술 취약점 혹은 통제에 관해 알지 못한다. 따라서 리스크 평가는 시스템에 대한 높은 수준의 리스크를 식별하고 분석하는 데 초점을 맞춰야 한다. 리스크 평가 프로세스의 결과는 보안성 요구사항을 식별하는 데 사용된다.
2. **설계 리스크 평가**: 이 리스크 평가는 시스템 개발 생명주기 동안에 행해지고 기술적인 시스템 설계 및 구현 결정에 영향을 받는다. 이 평가의 결과는 보안성 요구사항의 변경과 새로운 요구사항의 추가를 초래할 수 있다. 알려진 잠재적인 취약점이 인식되고 나서 이러한 지식이 시스템 기능과 기능의 구현, 테스트, 배치 방법에 관한 의사결정에 정보를 제공하는 데 이용된다.
3. **운영 리스크 평가**: 이 리스크 평가 프로세스는 시스템의 사용과 발생 가능한 리스크에 초점을 맞춘다. 예를 들어, 인터럽트가 자주 발생하는 환경에서 시스템이 사용되는 경우에 보안 리스크는 로그인한 사용자가 인터럽트를 처리하기 위해 그들의 컴퓨터를 무인상태로 놓아두는 것이다. 이 리스크에 대해 대항하기 위해, 일정 비활동 시간 후에 사용자가 자동적으로 로그아웃될 수 있도록 타임아웃 요구사항을 명시할 수 있다.

📘 (**396p 13.2.1 보안성 리스크 평가**)

보안 리스크 분석이 기술적이기 보다는 사업적인 이유
📘 **(396p)**

- 공격의 일부 유형이 기술 기반이 아니라 더 일반적인 조직 보안 취약점에 의존하기 때문이다.
- ex) 공격자가 승인 받은 엔지니어처럼 행동하면서 장비에 접근 할 수 있다.

제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾

📘 **(395p.)**

보안 정책을 말해 보시오.

- 조직 전체에 걸쳐 적용되는 일반적인 정보 접근 전략을 명시한다.

보안 정책의 요지는 왜 간단하게 적어야 하는지 말해 보시오.

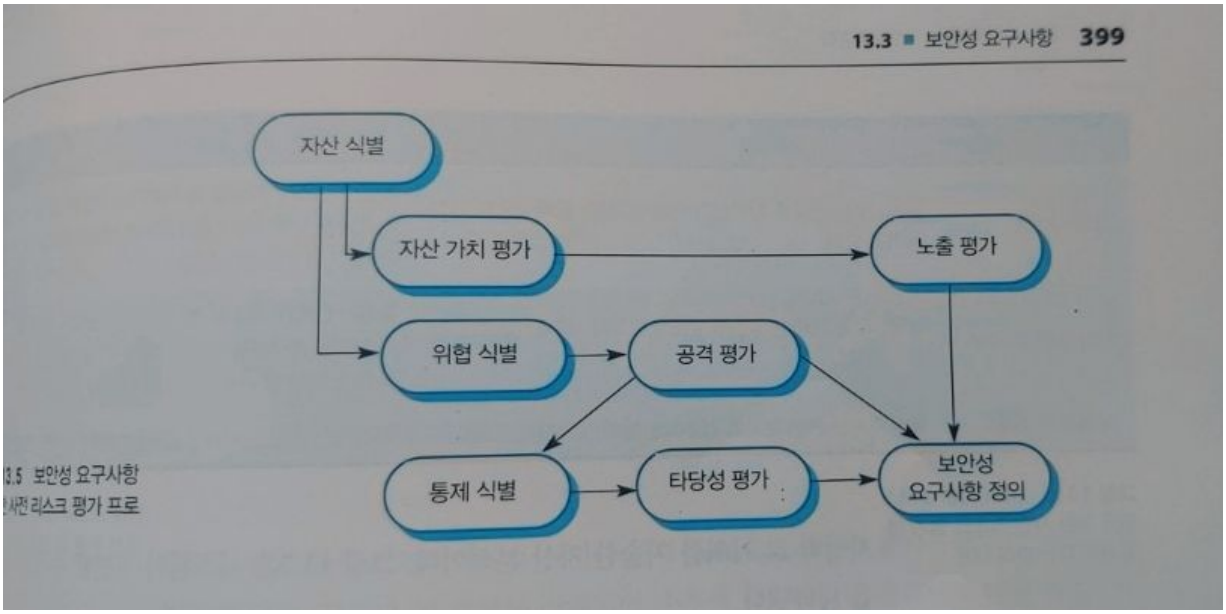
- 보안 정책의 요점은 조직 내의 모든 사람에게 보안에 대해 알리는 것이므로 길고 자세하면 안된다.

보안 목표를 말해 보시오.

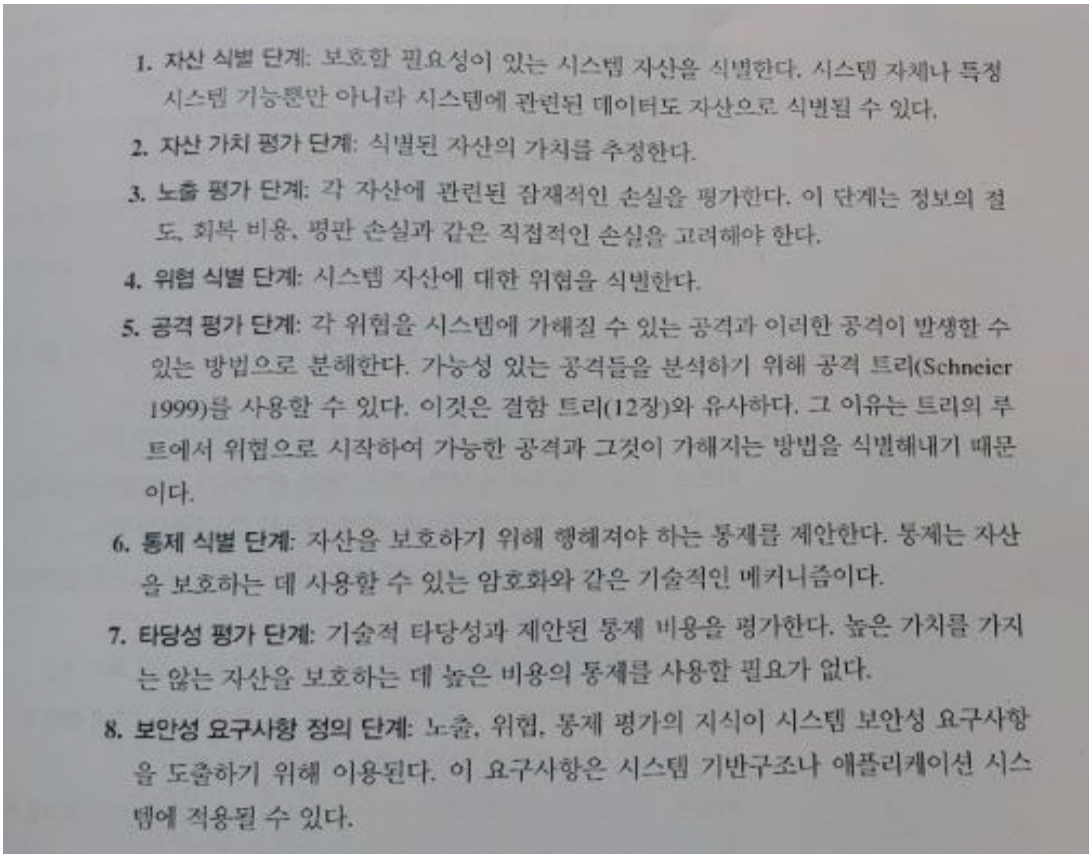
- 보안성 공학 관점에서 보안 정책은 광범위한 용어로 조직의 보안 목표를 정의한다.

📘 **(399p.)**

보안 공학 프로세스를 말해 보시오.

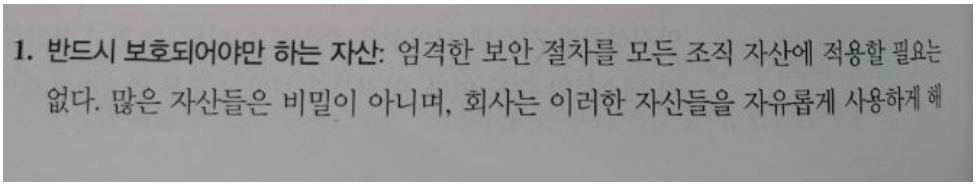


제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾



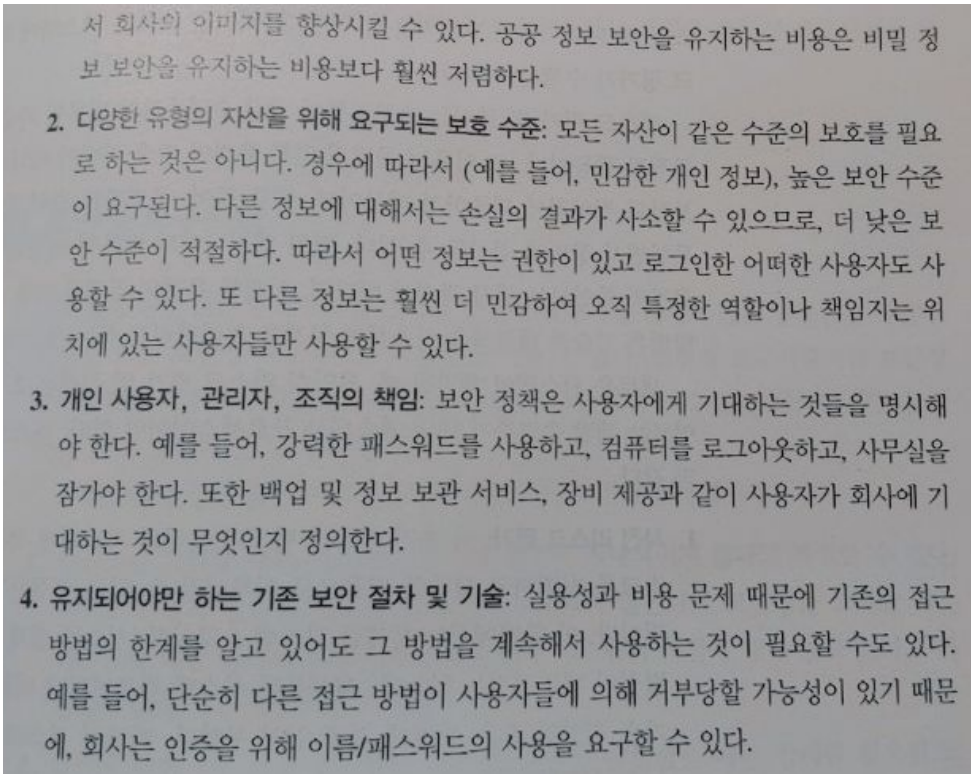
1. **자산 식별 단계**: 보호할 필요성이 있는 시스템 자산을 식별한다. 시스템 자체나 특정 시스템 기능뿐만 아니라 시스템에 관련된 데이터도 자산으로 식별될 수 있다.
2. **자산 가치 평가 단계**: 식별된 자산의 가치를 추정한다.
3. **노출 평가 단계**: 각 자산에 관련된 잠재적인 손실을 평가한다. 이 단계는 정보의 절도, 회복 비용, 평판 손실과 같은 직접적인 손실을 고려해야 한다.
4. **위협 식별 단계**: 시스템 자산에 대한 위협을 식별한다.
5. **공격 평가 단계**: 각 위협을 시스템에 가해질 수 있는 공격과 이러한 공격이 발생할 수 있는 방법으로 분해한다. 가능성 있는 공격들을 분석하기 위해 공격 트리(Schneier 1999)를 사용할 수 있다. 이것은 결함 트리(12장)와 유사하다. 그 이유는 트리의 루트에서 위협으로 시작하여 가능한 공격과 그것이 가해지는 방법을 식별해내기 때문이다.
6. **통제 식별 단계**: 자산을 보호하기 위해 행해져야 하는 통제를 제안한다. 통제는 자산을 보호하는 데 사용할 수 있는 암호화와 같은 기술적인 메커니즘이다.
7. **타당성 평가 단계**: 기술적 타당성과 제안된 통제 비용을 평가한다. 높은 가치를 가지는 않는 자산을 보호하는 데 높은 비용의 통제를 사용할 필요가 없다.
8. **보안성 요구사항 정의 단계**: 노출, 위협, 통제 평가의 지식이 시스템 보안성 요구사항을 도출하기 위해 이용된다. 이 요구사항은 시스템 기반구조나 애플리케이션 시스템에 적용될 수 있다.

보안 정책의 네 가지 원리



1. **반드시 보호되어야만 하는 자산**: 엄격한 보안 절차를 모든 조직 자산에 적용할 필요는 없다. 많은 자산들은 비밀이 아니며, 회사는 이러한 자산들을 자유롭게 사용하게 해

제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾



서 회사의 이미지를 향상시킬 수 있다. 공공 정보 보안을 유지하는 비용은 비밀 정보 보안을 유지하는 비용보다 훨씬 저렴하다.

2. **다양한 유형의 자산을 위해 요구되는 보호 수준**: 모든 자산이 같은 수준의 보호를 필요로 하는 것은 아니다. 경우에 따라서 (예를 들어, 민감한 개인 정보), 높은 보안 수준이 요구된다. 다른 정보에 대해서는 손실의 결과가 사소할 수 있으므로, 더 낮은 보안 수준이 적절하다. 따라서 어떤 정보는 권한이 있고 로그인한 어떠한 사용자도 사용할 수 있다. 또 다른 정보는 훨씬 더 민감하여 오직 특정한 역할이나 책임지는 위치에 있는 사용자들만 사용할 수 있다.
3. **개인 사용자, 관리자, 조직의 책임**: 보안 정책은 사용자에게 기대하는 것들을 명시해야 한다. 예를 들어, 강력한 패스워드를 사용하고, 컴퓨터를 로그아웃하고, 사무실을 잠가야 한다. 또한 백업 및 정보 보관 서비스, 장비 제공과 같이 사용자가 회사에 기대하는 것이 무엇인지 정의한다.
4. **유지되어야만 하는 기존 보안 절차 및 기술**: 실용성과 비용 문제 때문에 기존의 접근 방법의 한계를 알고 있어도 그 방법을 계속해서 사용하는 것이 필요할 수도 있다. 예를 들어, 단순히 다른 접근 방법이 사용자들에 의해 거부당할 가능성이 있기 때문에, 회사는 인증을 위해 이름/패스워드의 사용을 요구할 수 있다.

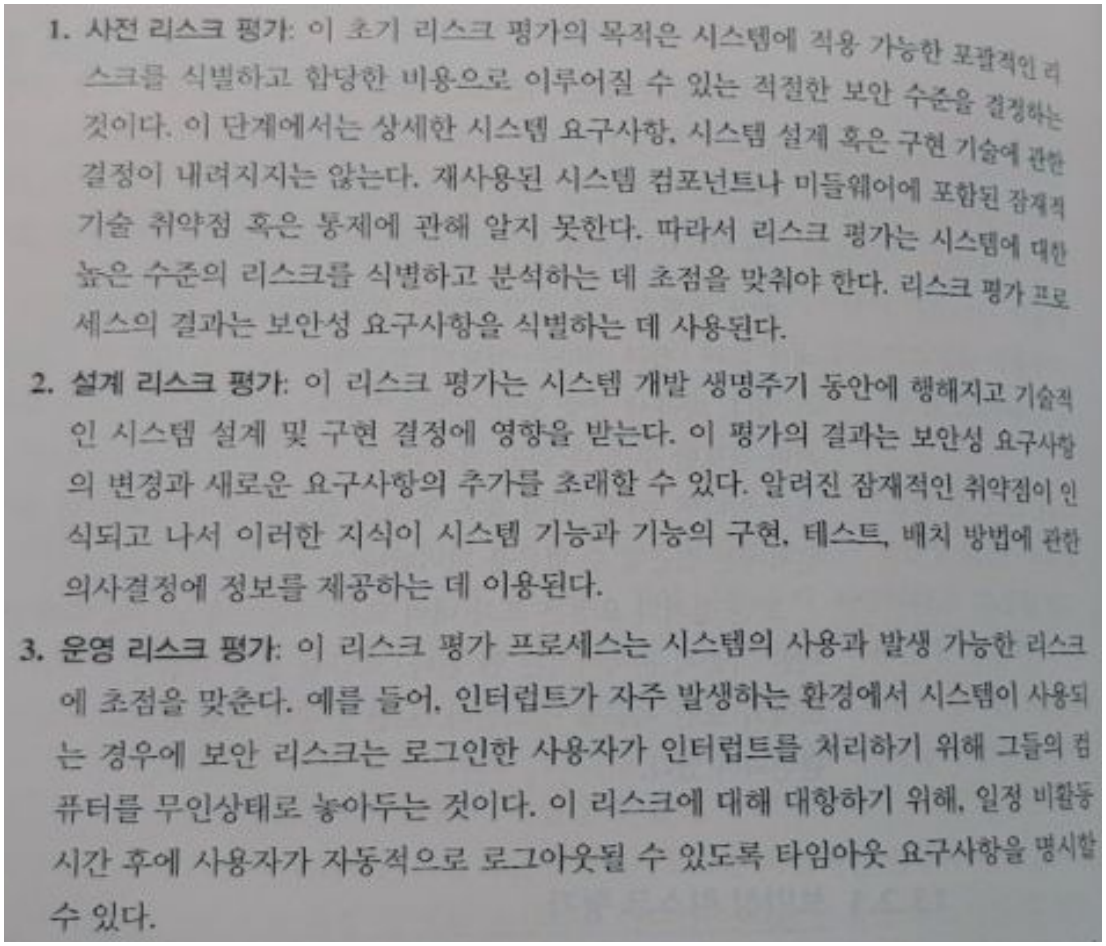
리스크 평가와 관리

리스크 평가는 왜 보안 정책에 의해 주도되어야 하는지

세 가지 리스크 관리 활동📘 (396p.)

- 사전 리스크 평가
- 설계 리스크 평가
- 운영 리스크 평가

제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾



1. **사전 리스크 평가**: 이 초기 리스크 평가의 목적은 시스템에 적용 가능한 포괄적인 리스크를 식별하고 합당한 비용으로 이루어질 수 있는 적절한 보안 수준을 결정하는 것이다. 이 단계에서는 상세한 시스템 요구사항, 시스템 설계 혹은 구현 기술에 관한 결정이 내려지지는 않는다. 재사용된 시스템 컴포넌트나 미들웨어에 포함된 잠재적 기술 취약점 혹은 통제에 관해 알지 못한다. 따라서 리스크 평가는 시스템에 대한 높은 수준의 리스크를 식별하고 분석하는 데 초점을 맞춰야 한다. 리스크 평가 프로세스의 결과는 보안성 요구사항을 식별하는 데 사용된다.
2. **설계 리스크 평가**: 이 리스크 평가는 시스템 개발 생명주기 동안에 행해지고 기술적인 시스템 설계 및 구현 결정에 영향을 받는다. 이 평가의 결과는 보안성 요구사항의 변경과 새로운 요구사항의 추가를 초래할 수 있다. 알려진 잠재적인 취약점이 인식되고 나서 이러한 지식이 시스템 기능과 기능의 구현, 테스트, 배치 방법에 관한 의사결정에 정보를 제공하는 데 이용된다.
3. **운영 리스크 평가**: 이 리스크 평가 프로세스는 시스템의 사용과 발생 가능한 리스크에 초점을 맞춘다. 예를 들어, 인터럽트가 자주 발생하는 환경에서 시스템이 사용되는 경우에 보안 리스크는 로그인한 사용자가 인터럽트를 처리하기 위해 그들의 컴퓨터를 무인상태로 놓아두는 것이다. 이 리스크에 대해 대항하기 위해, 일정 비활동 시간 후에 사용자가 자동적으로 로그아웃될 수 있도록 타임아웃 요구사항을 명시할 수 있다.

📖 책 참고내용

제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾

😎 보안 요구사항

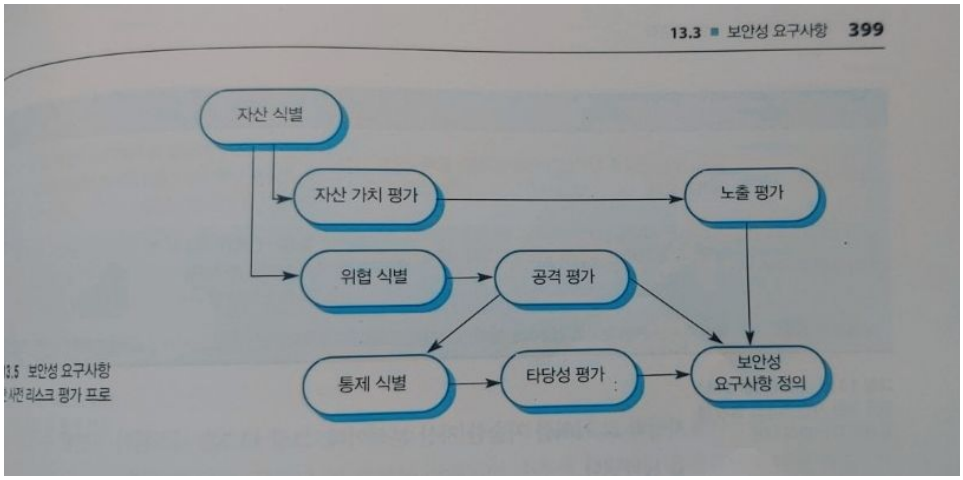
📌💾 ppt 참고내용

안전성 요구사항과 보안성 요구사항의 유사점을 말해 보시오.
- 둘 다 뭔가 나쁜일이 일어나는 것을 피하기 위함이다.

📘 **(397p.)**
안전성 요구사항과 보안성 요구사항의 차이점을 말해 보시오
- 안전은 사고적이라면 보안은 고의적이다. 공격자들이 약한 부분을 알고 공격해온다,.
- 보안은 공격자들이 이유를 숨겨서 발생원인을 모르게 한다.
- 안전사고가 나면 Shut down을 하는데 이게 공격자의 의도에 말려들어가는 것일 수 있다..
- 안전은 우연한 사고지만 보안은 매우 지능적인 공격자로부터

📌보안 요구 사항의 세가지 분류를 말해 보시오.(📣**교수님 | 시험에 나왔다)**
📘 **(398p.)**

리스크 회피 요구사항	요구 사항은 피해야 할 위험을 설정합니다 이러한 위험이 발생하지 않도록 시스템을 설계합니다. 리스크가 발생하지 않도록 시스템을 설계하여 리스크를 회피한다.
리스크 감지 요구사항	리스크가 발생하면 이를 식별하고 손실이 발생하기 전에 리스크를 무효화시키는 매커니즘을 정의한다.
리스크 완화 요구사항	손실이 발생한 후에 이로부터 회복하고 시스템 자산을 복구하기 위해 시스템이 어떻게 설계 되어야 하는 지 명시한다



제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾

📘 **(399p.)**
보안 위험 평가 활동인 "**자산 식별**", "**자산 가치 평가**", "**노출 평**가", "위**협 식별**", "**공격 평가**", "**대책 식별**", **타당성 평가**", "**보안 요구사항 정의**"를 말해 보시오.

자산 식별 Asset identification	보호할 필요성이 있는 시스템 자산을 식별한다. 시스템 자체나 특정 시스템 기능뿐만 아니라 시스템에 관련된 데이터도 자산으로 식별될 수 있다.
자산 가치 평가 Asset value assessment	식별된 자산의 가치를 추정한다.
노출평가 Exposure assessment	각각과 관련된 잠재적 손실을 평가
위협식별 Threat identification	시스템 자산에 대한 위협을 식별한다.
공격 평가 Attack assessment	위협을 가능한 공격으로 분해 시스템 및 이러한 상황이 발생할 수있는 방법.
대책 식별 Control identification	제정 될 수있는 통제를 제안 자산을 보호하십시오.
타당성 평가 Feasibility assessment	
보안 요구사항 정의 Security requirements definition	

오용 케이스를 말해 보시오.

- **차단 위협 (Interception threats) :** 공격자가 자산에 액세스합니다. ·
- **중단 위협(Interruption threats) :** 공격자가 시스템의 일부를 사용할 수 없게합니다.
- **수정 위협(Modification threat) :** 변조 된 시스템 자산
- **제조 위협(Fabrication threats) :** 시스템에 잘못된 정보가 추가됨

제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾

📖 책 참고내용

제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️ ppt: 💾

😎 보안 시스템 설계

📖 책 참고내용

📌💾 ppt 참고내용
보안은 왜 미리 설계해야 하는지 말해 보시오. • **디자인되고 구현된** 📘 **(405p.)** **보안을 추가하면 성능과 보안성에 어떤 영향을 주는지 말해 보시오.** **이미지** 📘 **(399p.) 서로 겹치는 설계 및 리스크 평가** **설계 리스크 평가를 말해 보시오.** **아키텍처 설계시 고려해야 할 두 가지 핵심적인 사항을 말해 보시오.** • **보호** • **분산** **계층화를 통해 해결** 📌 보호에 대해 말해 보시오.(📣**교수님 | 시험에 나왔다)** • 보호 ◦ 시스템이 어떻게 구성되어야 중요한 자산이 외부 공격으로부터 보호될 수 있는가? **분산에 대해 말해 보시오.** • 분산 ◦ 시스템 자산이 어떻게 분산되어야 성공적인 공격의 결과를 최소화할 수 있는가? **보호와 분산간의 충돌에 대해 말해 보시오.** • 이들은 잠재적으로 충돌합니다. 자산이 분산되면 보호하는데 더 많은 비용이 듭니다. • 여러겹의 보호계층을 만들게 되면 강력한 보안을 유지 할 수 있으나 **시스템 사용성에 영향**을 **성능 요구사항을 충족시키기 어려워진다**

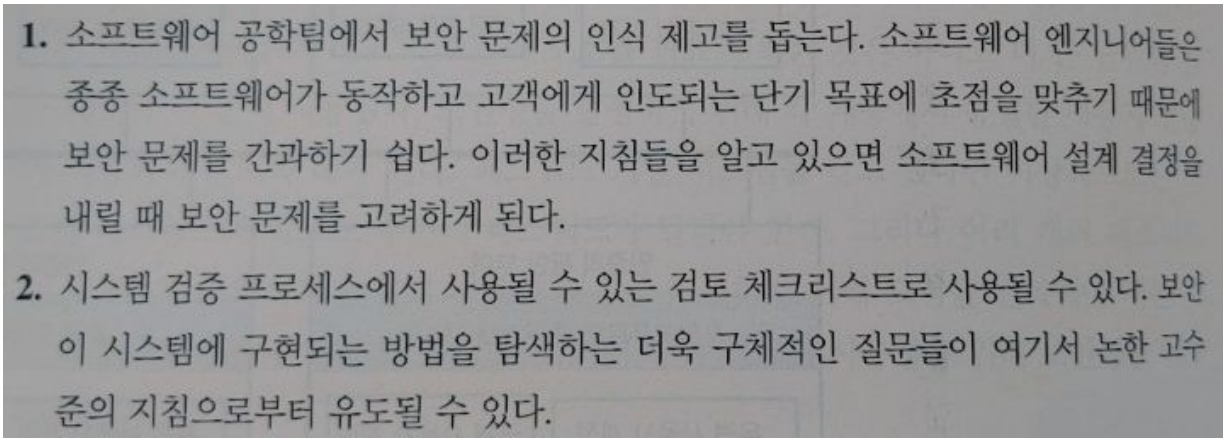
제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾

😎 보안 엔지니어링을위한 설계 지침

📌💾 ppt 참고내용

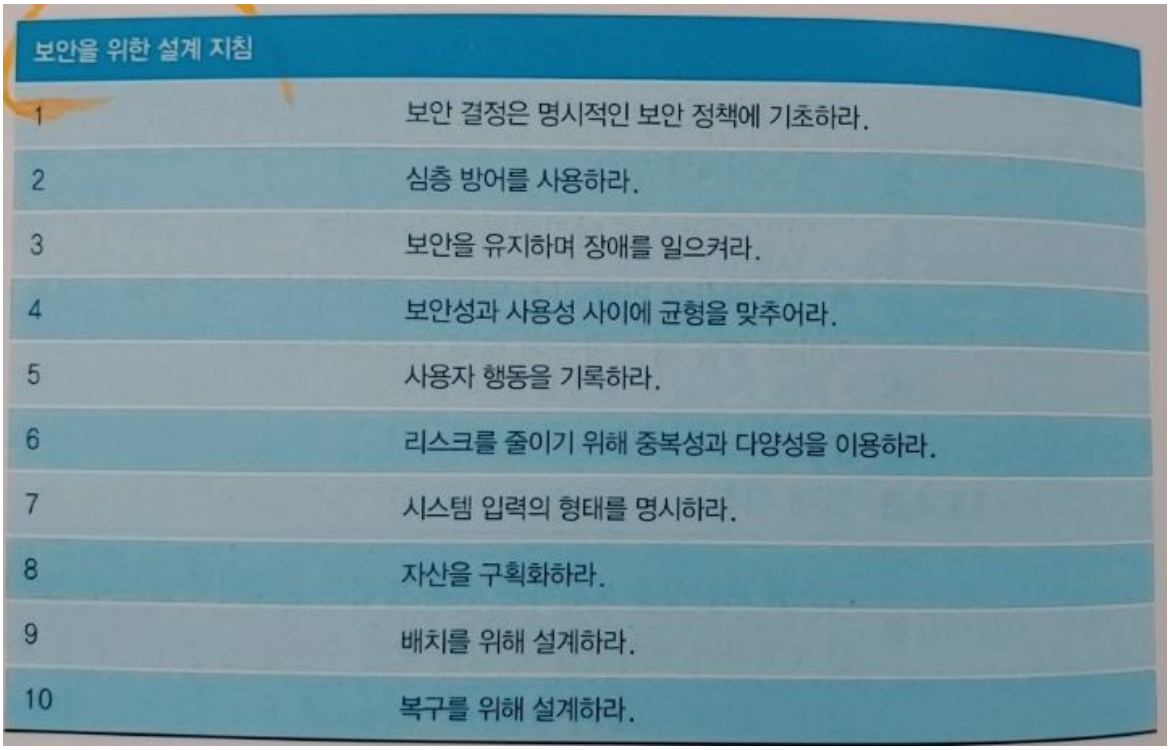
설계 가이드라인 또는 설계 지침이 무엇인지 말해 보시오.

📘 **(412p.)**
설계 지침의 두 가지 목적에 대해 말해 보시오.



1. 소프트웨어 공학팀에서 보안 문제의 인식 제고를 돕는다. 소프트웨어 엔지니어들은 종종 소프트웨어가 동작하고 고객에게 인도되는 단기 목표에 초점을 맞추기 때문에 보안 문제를 간과하기 쉽다. 이러한 지침들을 알고 있으면 소프트웨어 설계 결정을 내릴 때 보안 문제를 고려하게 된다.
2. 시스템 검증 프로세스에서 사용될 수 있는 검토 체크리스트로 사용될 수 있다. 보안이 시스템에 구현되는 방법을 탐색하는 더욱 구체적인 질문들이 여기서 논한 고수준의 지침으로부터 유도될 수 있다.

📘 **(412p. - 책에 자세히 나와있음)**
보안을 위한 10 개 지침을 말해 보시오.



보안을 위한 설계 지침	
1	보안 결정은 명시적인 보안 정책에 기초하라.
2	심층 방어를 사용하라.
3	보안을 유지하며 장애를 일으켜라.
4	보안성과 사용성 사이에 균형을 맞추어라.
5	사용자 행동을 기록하라.
6	리스크를 줄이기 위해 중복성과 다양성을 이용하라.
7	시스템 입력의 형태를 명시하라.
8	자산을 구획화하라.
9	배치를 위해 설계하라.
10	복구를 위해 설계하라.

📘 **(412p.) 보안성 있는 시스템 공학을 위한 설계 지침**

제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️ ppt: 💾

😃 복원성 공학(Resilience Engineering)

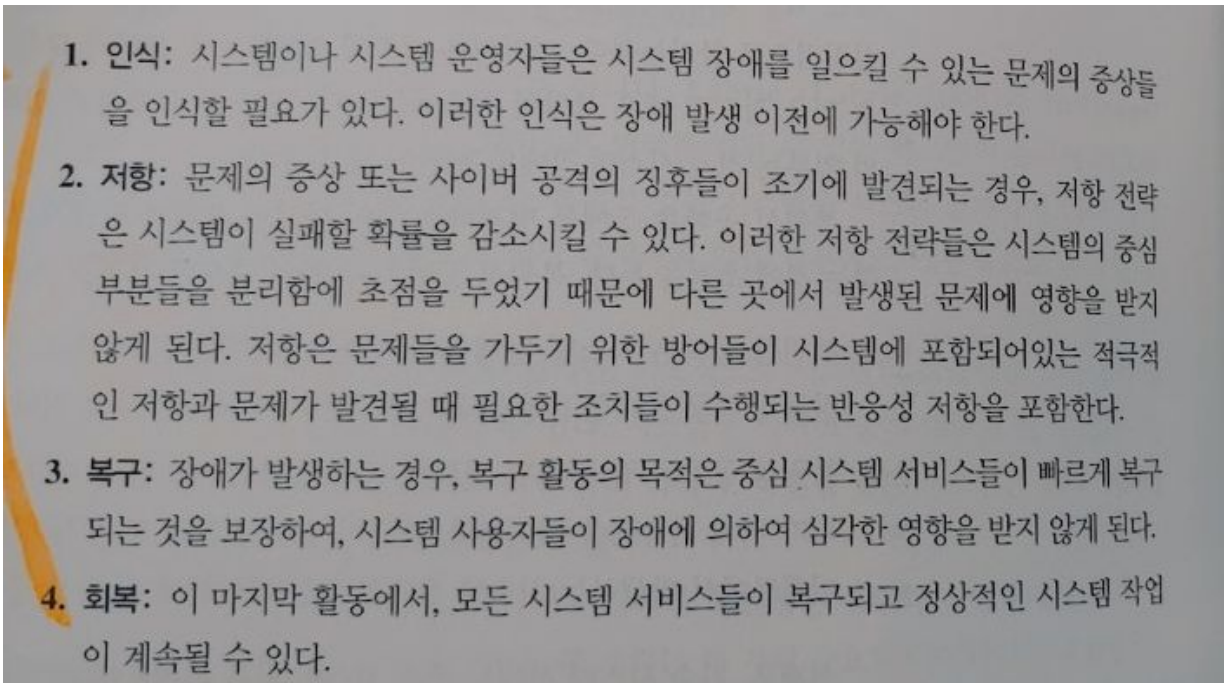
😎 개요

📖 책 참고내용

📌💾 ppt 참고내용
시스템 복원성을 말해 보시오. ● 중요한 서비스는 장애가 발생했음에도 불구하고 핵심 서비스가 얼마나 지속될 수 있는가의 정도 📘 **(426p.)** **복원성을 위한 세 가지 아이디어를 말해 보시오.** 1. 시스템에 의하여 제공되는 서비스들 중 일부의 장애가 인간, 사회, 그리고 경제적으로 심각한 영향을 발생시킬 수 있는 중심 서비스라는 아이디어 2. 일부의 이벤트는 파괴적이며 중심 서비스를 제공하는 시스템의 능력에 영향을 미칠 수 있다는 아이디어 3. 복원성은 판단이라는 아이디어. 즉 복원성에는 척도가 없고, 측정될 수도 없다. 시스템의 복원성은 시스템과 운영 프로세스를 감사할 수 있는 전문가에 의해서만 평가될 수 있다. **복원성 공학은 장애를 완전히 없애기 보다는 장애의 수를 줄이는 것을 강조한다는 말의 의미를 얘기해 보시오** ● 모든 시스템의 장애를 없애는 것은 불가능하다. 📘 **(427p.)** **두 가지 가정을 말해 보시오.** 1. 복원성 공학은 시스템 장애를 방지하는 것은 불가능하다고 가정하므로, 이러한 **고장들과 복구에 대한 비용을 최소화하는 것에 초점**을 두고 있다. 2. 복원성 공학은 잘 준비된 신뢰성 공학 경험이 시스템의 기술적 결함 수를 최소화시키기 위해 사용됨을 의미한다. 따라서 **잘못된 운영 또는 사이버 공격과 같은 외부적 이벤트에서 발생하는 시스템 장애의 수를 제한함에 더 많은 중점을 둔다.**

제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾

📌 **네 가지 복원성 활동(4R) 인식, 저항, 복구, 회복을 말해 보시오..**
📘 **(428p.)**



1. **인식:** 시스템이나 시스템 운영자들은 시스템 장애를 일으킬 수 있는 문제의 증상들을 인식할 필요가 있다. 이러한 인식은 장애 발생 이전에 가능해야 한다.
2. **저항:** 문제의 증상 또는 사이버 공격의 징후들이 조기에 발견되는 경우, 저항 전략은 시스템이 실패할 확률을 감소시킬 수 있다. 이러한 저항 전략들은 시스템의 중심 부분들을 분리함에 초점을 두었기 때문에 다른 곳에서 발생된 문제에 영향을 받지 않게 된다. 저항은 문제들을 가두기 위한 방어들이 시스템에 포함되어있는 적극적인 저항과 문제가 발견될 때 필요한 조치들이 수행되는 반응성 저항을 포함한다.
3. **복구:** 장애가 발생하는 경우, 복구 활동의 목적은 중심 시스템 서비스들이 빠르게 복구되는 것을 보장하여, 시스템 사용자들이 장애에 의하여 심각한 영향을 받지 않게 된다.
4. **회복:** 이 마지막 활동에서, 모든 시스템 서비스들이 복구되고 정상적인 시스템 작업이 계속될 수 있다.

제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾

😎 사이버 보안

📖 책 참고내용

📌💾 ppt 참고내용
사이버 범죄를 말해 보시오. • 사이버 범죄는 네트워크 시스템의 불법 사용이며 가장 심각한 범죄 중 하나입니다. **사이버 보안과 보안성 공학 관계의 관계를 말해 보시오** • 보안성 공학보다 광범위한 문제다. **보안성 공학**은 **시스템은 안전하다는 것을 보증하는 기법과 기술들에 초점을 맞춘 기본적 기술활동** • **사이버보안**은 **컴퓨터와 인터넷의 사용에서 발생하는 위협으로부터 시민 비즈니스 중심 기반구조들의 보호를 보증하는 모든 측면**을 포함한다. **사이버 보안은 왜 사회기술적 관심사인지 말해 보시오.** • **사이버 보안은 왜 조직의 모든 자산과 관련 있는지 말해 보시오.** 📘 **(429p.)** **사이버 보안의 실패 요인을 말해 보시오.** • 문제의 심각성에 대한 조직의 무지 • 보안 절차의 부실한 설계와 방만한 애플리케이션 • 사람의 부주의 • 사용성과 보안성 사이의 부적절한 절충 **사이버 보안의 위협을 말해 보시오.** • 기밀성 • 무결성 • 가용성

제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ☆ 📖 솔루션:💡 📘✔️
ppt: 💾

📘 **(431p.)**
자산을 보호하기 위한 보호 조치의 예를 설명 하시오.

- 인증 **Authentication**
  - 시스템 사용자가 시스템의 접근에 대한 권한을 보여준다. 인증을 위해 일반적으로 친숙한 로그인/암호 접근법이 사용되지만, **약한 보안 방법이다.**
- 암호화 **Encryption**
  - 인증받지 못한 독자가 정보에 접근할 수 없도록 데이터를 알고리즘으로 뒤섞는다. 많은 기업들이 이제 암호화된 노트북 디스크를 요구하고 있다. 컴퓨터가 분실되었거나 도난당한 경우, 암호화는 정보의 기밀성이 위반될 가능성을 감소시킨다.
- 방화벽 **Firewalls**
  - 수신 네트워크 패킷을 검사하여 조직에서 정의한 규칙들에 따라 패킷을 허용하거나 또는 거부한다. 방화벽은 신뢰할 수 있는 송신자로부터의 트래픽만이 외부 인터넷으로부터 조직의 내부 네트워크로 전달되는 것을 허용한다.

📘 **(431~432p.)**
중복성과 다양성이 사이버보안 복원에 왜 중요한지 말해 보시오.

1. 각 시스템에서, 데이터와 소프트웨어의 복제본은 별도의 컴퓨터 시스템에서 유지되어야 한다. 가능하면 공유 디스크를 피해야 한다. 이것은 사이버 공격이 발생한 이후 복구를 효율적으로 지원한다.**(복구의 회복)**

2. 다양한 다단계 인증은 암호 공격을 보호할 수 있다. ID/PW 인증뿐만 아니라, 사용자에게 개인 정보나 모바일 폰으로 생성된 코드를 제공하도록 하는 추가 인증 단계들이 포함될 수 있다.**(저항)**

3. 더 많은 수의 중심 서버들을 구입할 수 있다. 즉 예상되는 부하를 처리하기 위해 요구된 것보다 시스템이 더 많은 용량을 가질 수 있다. 여분의 자원은 서버의 정상적 반응 시간이 감소될 필요 없이 공격에 저항할 수 있다는 것을 의미한다. 따라서 다른 서버들이 손상된 경우, 여분의 자원들은 그들이 수리되는 동안 소프트웨어를 실행하는데 활용된다.**(저항과 복구)**

제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾

📘 **(432p.)**

사이버 복원 계획의 6가지 주요 활동

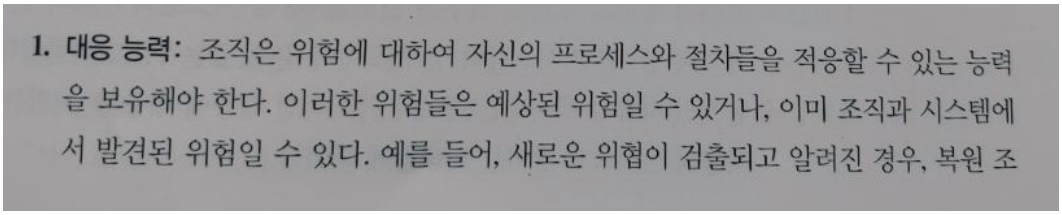
1. **자산 분류:** 조직의 하드웨어, 소프트웨어 및 인적 자산들은 그들이 정상 작동에 얼마나 중요한가에 따라 검토되고 분류된다. 자산들은 중심(critical), 중요(important) 또는 유용한(useful) 자산으로 분류될 수 있다.
2. **위협 식별:** 각 자산(적어도 중심 자산과 중요 자산)에 대해, 각 자산에 대한 위협을 식별하고 분류해야 한다. 위협이 발생할 확률을 예측해야 하지만, 어떤 경우에는 잠재적인 공격자에 대한 충분한 정보가 없기 때문에 이러한 예측은 종종 부정확할 수도 있다.
3. **위협 인식:** 각 위협 또는 자산/위협 쌍에 대해, 위협에 따른 공격이 인식되는 방법을 식별해야 한다. 위협의 인식을 위해 추가적인 소프트웨어가 구입되거나 작성되어야 할 필요성 또는 정기적 검사 절차가 수행되어야 할 필요성을 결정해야 한다.
4. **위협 저항:** 각 위협 또는 자산/위협 쌍에 대해, 가능한 저항 전략을 식별해야 한다. 시스템에 포함될 수 있고 또는 운영 절차에 의지할 수도 있다. 위협 중립화 전략을 고려해서 위협이 재발하지 않도록 고려할 필요가 있다.
5. **자산 복구:** 각 중심 자산 또는 자산/위협 쌍에 대해, 사이버 공격이 발생하는 경우 해당 자산을 복구할 방법을 수행해야 한다. 이것은 데이터를 중복시킨 복제본에 쉽게 접근하기 위해 추가 하드웨어를 준비하거나 백업 절차를 변경하는 것을 포함할 수 있다.
6. **자산 회복:** 시스템이 다시 정상적으로 운영되기 위한 절차들을 정의하는 자산 복구의 보다 일반적인 과정이다. 자산 회복은 간단한 자산이 아닌 조직의 중요한 모든 자산들을 다루어야 한다.

제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾

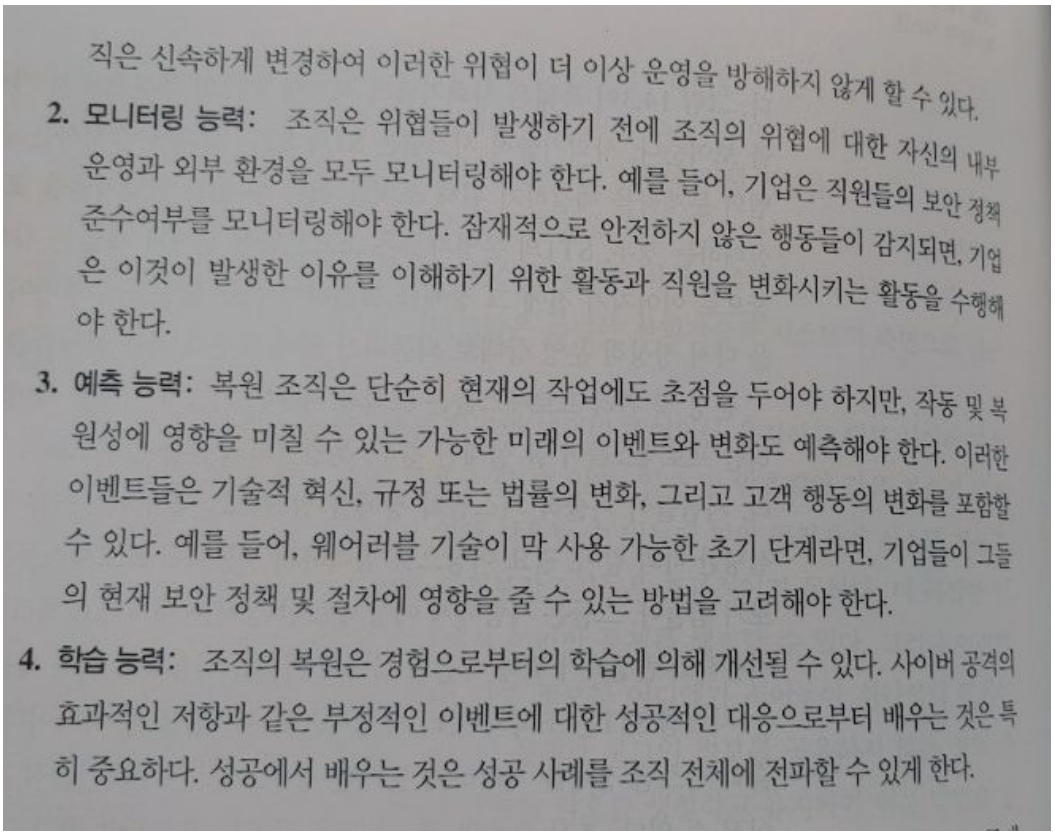
😎 사회 기술 복원력

📌💾 ppt 참고내용
복원성 공학이 관심 갖는 악의적인 외부 이벤트를 말해 보시오. • **복원성있는 시스템을 설계하기 위해서는 소프트웨어만 고려해서는 안 되는 이유를 말해 보시오.** • 복원성 공학은 시스템장애로 이어질 수 있는 악의적인 외부 이벤트를 고려해야 한다 • 이런 이벤트들은 사회기술적 시스템 측면으로 접근하면 어떤 이벤트가 발생할지 알 수 없기 때문에 넓은 사회기술적 시스템을 고려해야 한다. **더 넓은 사회기술적 시스템을 고려해야 하는 이유를 말해 보시오.** • 시스템을 유연하고 적응성 있게 구축하여 그들이 예기치 못한 상황에 대처 할 수 있게 해야하기 때문 📘 **(435p.)** **조직의 복원성을 반영하는 네 가지 특징을 말해 보시오.**

제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾



1. **대응 능력:** 조직은 위험에 대하여 자신의 프로세스와 절차들을 적응할 수 있는 능력을 보유해야 한다. 이러한 위험들은 예상된 위험일 수 있거나, 이미 조직과 시스템에서 발견된 위험일 수 있다. 예를 들어, 새로운 위협이 검출되고 알려진 경우, 복원 조



직은 신속하게 변경하여 이러한 위협이 더 이상 운영을 방해하지 않게 할 수 있다.

2. **모니터링 능력:** 조직은 위협들이 발생하기 전에 조직의 위협에 대한 자신의 내부 운영과 외부 환경을 모두 모니터링해야 한다. 예를 들어, 기업은 직원들의 보안 정책 준수여부를 모니터링해야 한다. 잠재적으로 안전하지 않은 행동들이 감지되면, 기업은 이것이 발생한 이유를 이해하기 위한 활동과 직원을 변화시키는 활동을 수행해야 한다.

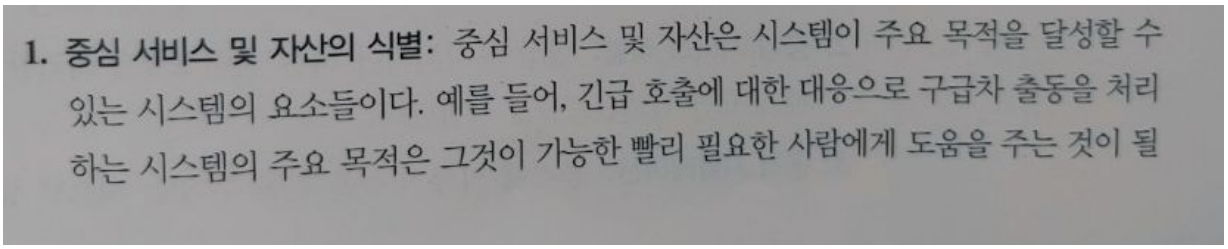
3. **예측 능력:** 복원 조직은 단순히 현재의 작업에도 초점을 두어야 하지만, 작동 및 복원성에 영향을 미칠 수 있는 가능한 미래의 이벤트와 변화도 예측해야 한다. 이러한 이벤트들은 기술적 혁신, 규정 또는 법률의 변화, 그리고 고객 행동의 변화를 포함할 수 있다. 예를 들어, 웨어러블 기술이 막 사용 가능한 초기 단계라면, 기업들이 그들의 현재 보안 정책 및 절차에 영향을 줄 수 있는 방법을 고려해야 한다.

4. **학습 능력:** 조직의 복원은 경험으로부터의 학습에 의해 개선될 수 있다. 사이버 공격의 효과적인 저항과 같은 부정적인 이벤트에 대한 성공적인 대응으로부터 배우는 것은 특히 중요하다. 성공에서 배우는 것은 성공 사례를 조직 전체에 전파할 수 있게 한다.

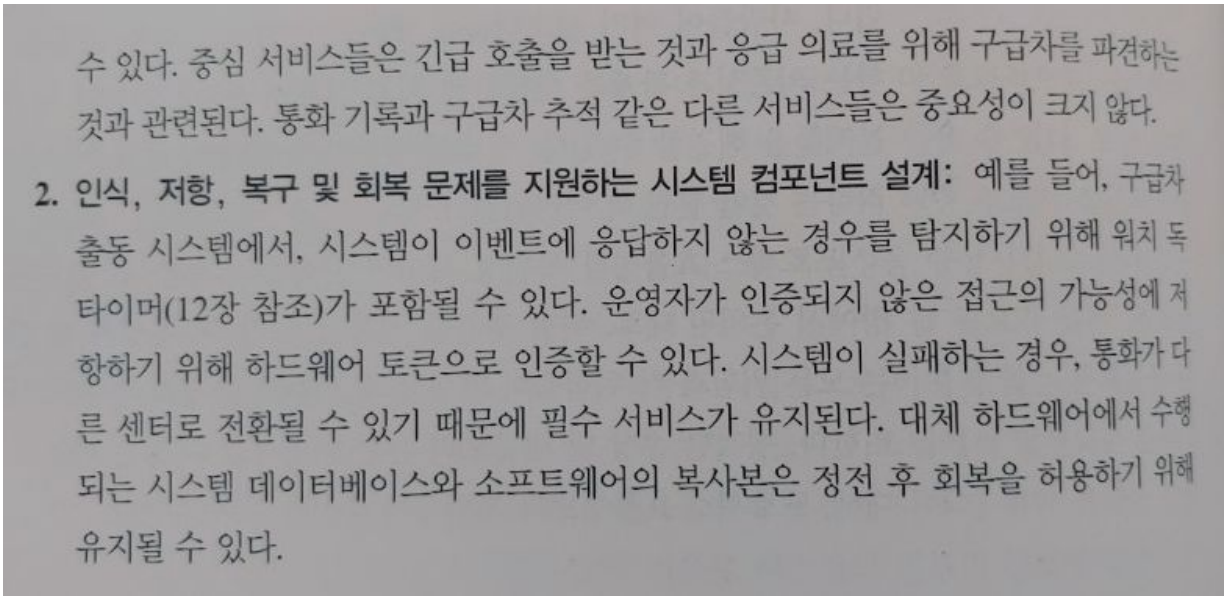
제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾

📘 **(436p.)**
인간 오류를 말해 보시오.

📘 **(437p.)**
인간 오류를 고려하는 두 가지 방식을 말해 보시오.



1. **중심 서비스 및 자산의 식별:** 중심 서비스 및 자산은 시스템이 주요 목적을 달성할 수 있는 시스템의 요소들이다. 예를 들어, 긴급 호출에 대한 대응으로 구급차 출동을 처리하는 시스템의 주요 목적은 그것이 가능한 빨리 필요한 사람에게 도움을 주는 것이 될



수 있다. 중심 서비스들은 긴급 호출을 받는 것과 응급 의료를 위해 구급차를 파견하는 것과 관련된다. 통화 기록과 구급차 추적 같은 다른 서비스들은 중요성이 크지 않다.

2. **인식, 저항, 복구 및 회복 문제를 지원하는 시스템 컴포넌트 설계:** 예를 들어, 구급차 출동 시스템에서, 시스템이 이벤트에 응답하지 않는 경우를 탐지하기 위해 워치 독 타이머(12장 참조)가 포함될 수 있다. 운영자가 인증되지 않은 접근의 가능성에 저항하기 위해 하드웨어 토큰으로 인증할 수 있다. 시스템이 실패하는 경우, 통화가 다른 센터로 전환될 수 있기 때문에 필수 서비스가 유지된다. 대체 하드웨어에서 수행되는 시스템 데이터베이스와 소프트웨어의 복사본은 정전 후 회복을 허용하기 위해 유지될 수 있다.

📘 **(437p.)**
인간 오류가 발생한다고 가정하는 이유를 말해 보시오.
- 사람은 늘 실수 할 수 있다.

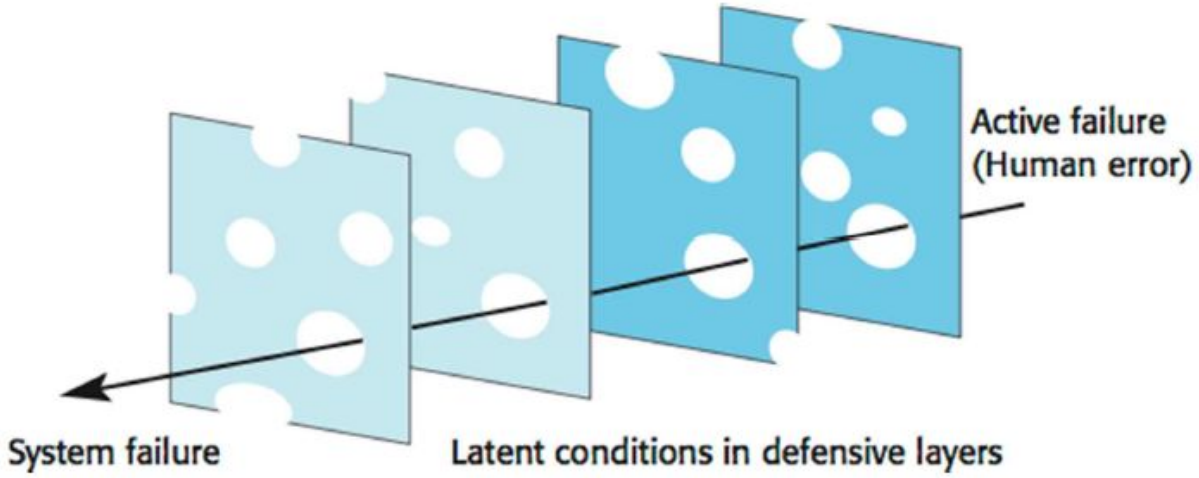
인간 오류에 대처하기 위한 방어와 장벽을 말해 보시오.
- 기술적인 장벽
- 사회적인 장벽

제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾

기술적 장벽을 말해 보시오.

사회기술적 장벽을 말해 보시오.

Reason 의 "스위스 치즈" 모델을 말해 보시오.



방어 장벽들이 취약점을 가질 때 어떤 일이 발생하는지 말해 보시오.

시스템 복원성을 향상시키는 전략을 말해 보시오.

- 시작은 잘만들자
- 방어수단을 더 만들자
- 방어수단을 다양한 방식으로 만들자
- 시스템에 있는 잠재되어 있는 결함의 수를 줄이자(치즈 구멍의 수를 최소화하자)

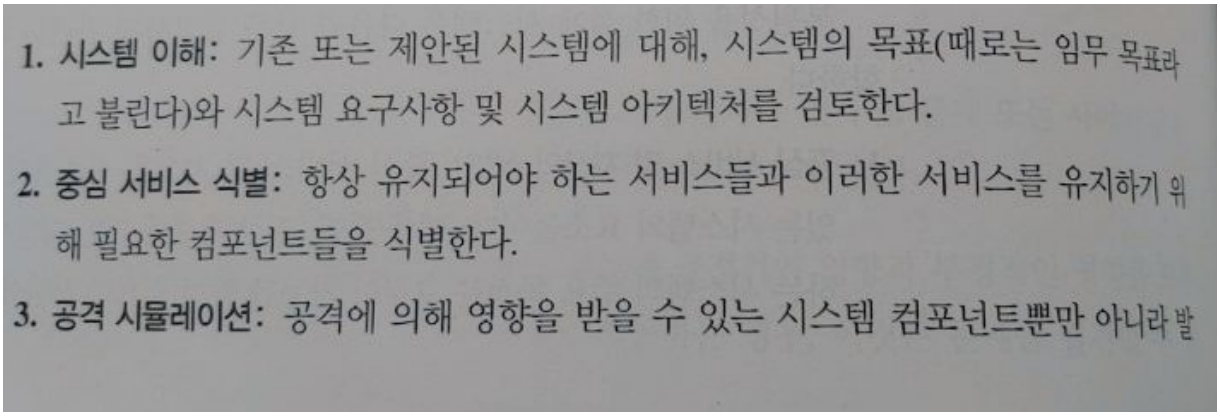
제목: 😃 부제목:😎 인덱스:📜 교수님:📣 쪽집게:📌 중요: 책참고: ⭐ 📖 솔루션:💡 📘✔️
ppt: 💾

😎 회복력있는 시스템 디자인

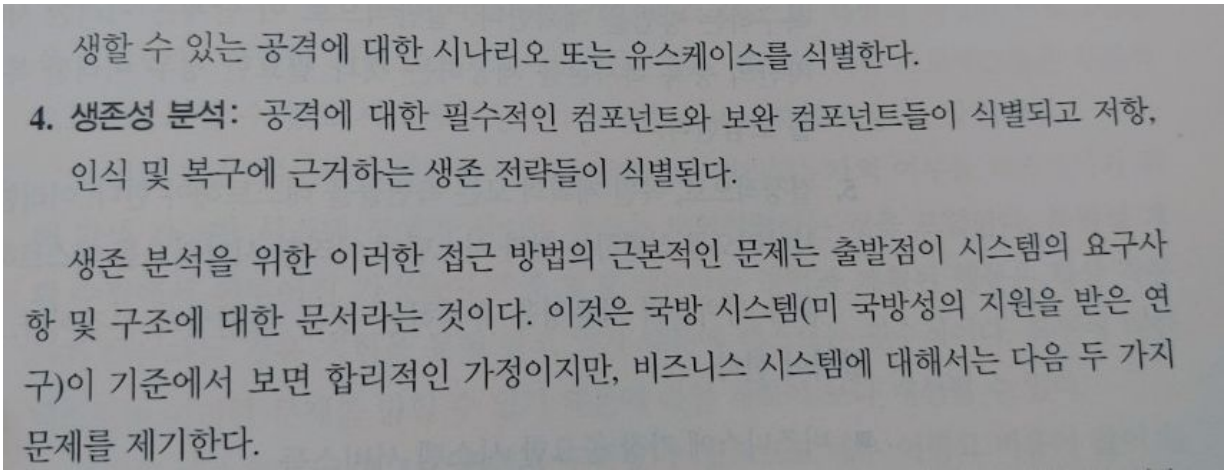
📌💾 ppt 참고내용

복원성있는 시스템을 설계하기 위한 두 가지 작업 흐름을 말해 보시오.

생존가능한 분석의 핵심 활동을 말해 보시오.



1. **시스템 이해:** 기존 또는 제안된 시스템에 대해, 시스템의 목표(때로는 임무 목표라고 불린다)와 시스템 요구사항 및 시스템 아키텍처를 검토한다.
2. **중심 서비스 식별:** 항상 유지되어야 하는 서비스들과 이러한 서비스를 유지하기 위해 필요한 컴포넌트들을 식별한다.
3. **공격 시뮬레이션:** 공격에 의해 영향을 받을 수 있는 시스템 컴포넌트뿐만 아니라 발



생할 수 있는 공격에 대한 시나리오 또는 유스케이스를 식별한다.

4. **생존성 분석:** 공격에 대한 필수적인 컴포넌트와 보완 컴포넌트들이 식별되고 저항, 인식 및 복구에 근거하는 생존 전략들이 식별된다.

생존 분석을 위한 이러한 접근 방법의 근본적인 문제는 출발점이 시스템의 요구사항 및 구조에 대한 문서라는 것이다. 이것은 국방 시스템(미 국방성의 지원을 받은 연구)이 기준에서 보면 합리적인 가정이지만, 비즈니스 시스템에 대해서는 다음 두 가지 문제를 제기한다.