

2주차 1차시 시스템보안의 개념과 요소

【학습목표】

1. 시스템보안의 개념을 설명할 수 있다.
2. 시스템보안의 요소들의 특징을 통해 구분할 수 있다.

학습내용1 : 시스템 보안의 개념

1. 시스템

1) 국어사전 : 필요한 기능을 실현하기 위하여 관련 요소를 어떤 법칙에 따라 조합한 집합체'

2) 영어사전 :

- 제도, 체제
- 체계, 시스템, 장치
- (하나의 기관으로 본) 몸 (동물 체내의) 계

* 일반적으로 시스템을 만나면 화자의 성향과 그 단어가 사용된 상황을 인식한 후 어떤 의미인지 판단하여야 함

2. 시스템의 요소

1) 하드웨어로는 모니터, 키보드, 메인 보드, 하드 디스크, 램메모리 등

2) 소프트웨어로는 운영체제, 데이터베이스, 웹 서비스

3) 시스템은 많은 요소를 포괄하고 있는 개념임

3. IT 분야에서 시스템이란?

1) 특정목적이 전제되어야 함

- 시스템의 예) 공학적 시스템과 인문학적 시스템의 차이점 비교 언급

2) 목적을 이루는 도구가 IT요소이어야 함

- 인문학적 시스템은 차이점이 있음

3) 보안에서 언급하는 시스템이란

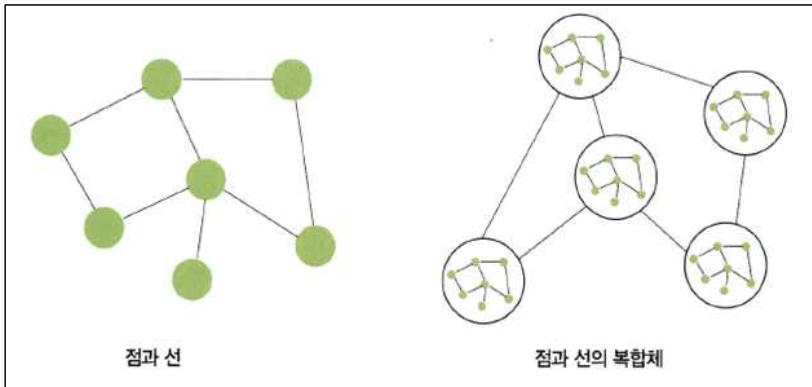
- 보안의 개념이 적용되는 목적을 가진 IT 시스템의 요소

4. 시스템 보안이란

- 1) 정보시스템을 구성하는 각 요소들이 가져야 할 보안의 겉옷
- 2) 시스템과 관련된 보안 주제는 어떠한 시스템에 한정되어 있는 것이 아니라 훨씬 큰 범위의 보안

예) 하나의 조직이나 국가 단위의 보안 요소와 매우 닮아 있다.

5. 시스템 보안의 이해



- 1) 인간 사회에서 한 사람의 개인이 점에 해당하고 사람들 간의 관계를 선이라고 생각한다면, 여러 사람이 모인 조직은 기업이나 국가가 되고, 다시 그것들을 연결하는 기업과 기업의 관계, 국가와 국가의 관계가 더 큰 형태의 점과 선이 된다.
- 2) 시스템의 계정과 권한 등의 보안 요소는 단순한 하나의 시스템(한사람)에 해당할 수도 있지만, 다양한 네트워크로 연결된 기업이나 국가의 시스템들이 점 하나가 될 수도 있다.
- 3) 시스템 보안은 권한 없는(허가받지 않은) 사용자에게 의한 파일, 폴더 및 장치 등의 사용을 제한하여 보호하는 시스템 기능을 말한다.

학습내용2 : 시스템 보안의 요소

1. 시스템 보안의 요소

- ① 계정과 패스워드 관리
- ② 세션 관리
- ③ 접근제어
- ④ 권한관리
- ⑤ 로그관리
- ⑥ 취약점관리

2. 계정과 패스워드 관리

- 적절한 권한을 가진 사용자를 식별하기 위한 가장 기본적인 인증 수단
- 시스템에서는 계정과 패스워드 관리가 보안의 시작
- 성에는 신분이 확실한 사람만 출입해야 함
- 계정과 패스워드는 주민의 신분증 및 외부인이 성을 방문할 때 보여주는 명령서 등의 공문서와 같은 역할을 한다.

3. 세션 관리

- 사용자와 시스템 또는 두 시스템 간의 활성화된 접속에 대한 관리
- 일정 시간이 지날 경우 적절히 세션을 종료하고, 비인가자에 의한 세션 가로채기를 통제
- 세션은 '사용자와 컴퓨터 또는 두 컴퓨터 간의 활성화된 접속'을 의미하는 것
- 외부인이 성 안에 머무를 수 있도록 허락해주는 기간으로 볼 수 있음
- 현대 사회에 서는 해외에 나갈 때 비자(Visa)를 받는데, 목적에 따라 기간이 명시되어 있는 비자가 이와 유사함

4. 접근제어

- 1) 시스템이 네트워크 안에서 다른 시스템으로부터 적절히 보호될 수 있도록 네트워크 관점에서 접근을 통제

- ① 신분증이나 공문서에 따라 접근 여부를 결정하는 과정이다.
- ② 어느 곳에서 온사람인지에 따라 성의 출입을 허용할 수도 있고 막을 수도 있는데, 이와 같은 과정이 접근 제어이다
- ③ 요즘에도 국가별로 출국을 막거나 허용하는 정책을 적용하고 있는데, 이 역시 접근제어라고 볼 수 있다.

5. 권한관리

- 1) 시스템의 각 사용자가 적절한 권한으로 적절한 정보 자산에 접근할 수 있도록 통제

- ① 성 안에서 물건을 사고 팔 수 있는 사람
- ② 높은 사람을 만날 수 있는 사람
- ③ 성을 지나갈 수만 있는 사람
- ④ 이주할 수 있는 사람으로 구분하는 것
- ⑤ 성에서 무엇에 접근할 수 있고 무엇을 할 수 있는지 통제하는 것과 유사하다

- 2) 시스템 내부 혹은 네트워크를 통한 외부에서 시스템에 어떤 영향을 미칠 경우 해당 사항을 기록

- ① 성 안에서 여러 가지 활동을 하다 보면 많은 내용이 기록된다.
- ② 성의 문지기는 성에 들어가고 나간 사람을 기록하고
- ③ 상인들은 누군가와 물건을 사고판 것을 기록하고
- ④ 여관에서는 숙박하는 사람들을 기록할 것이다.
- ⑤ 이런 것들이 시스템에서 로그와 같다.

6. 로그관리

- 시스템 내부 혹은 네트워크를 통한 외부에서 시스템에 어떤 영향을 미칠 경우 해당 사항을 기록
- ① 성 안에서 여러 가지 활동을 하다 보면 많은 내용이 기록됨
- ② 성의 문지기는 성에 들어가고 나간 사람을 기록
- ③ 상인들은 누군가와 물건을 사고판 것을 기록
- ④ 여관에서는 숙박하는 사람들을 기록할 것임
- ⑤ 이런 것들이 시스템에서 로그와 같음

7. 취약점관리

- 시스템은 계정과 패스워드 관리, 세션 관리, 접근 제어, 권한 관리 등을 충분히 잘 갖추고도 보안적인 문제가 발생할 수 있음.
- 이는 시스템 자체의 결함에 의한 것으로 이 결함을 체계적으로 관리하는 것이 취약점 관리이다.
- 성벽을 보수하는 일
- 위조된 신분증을 조사하고 조치하는 활동으로 볼 수 있다.

【학습정리】

1. 보안에서 언급하는 시스템이란 보안의 개념이 적용되는 목적을 가진 IT 시스템의 요소입니다.
2. 시스템보안이란 정보시스템을 구성하는 각 요소들이 가져야할 보안의 겉옷이며, 어떤 한 시스템에 한정되어 있는 것이 아니라 큰 범위의 보안을 말한다.
3. 시스템 보안의 요소로는 계정과 패스워드 관리, 세션 관리, 접근 제어, 권한 관리, 로그 관리, 취약점 관리가 있습니다.