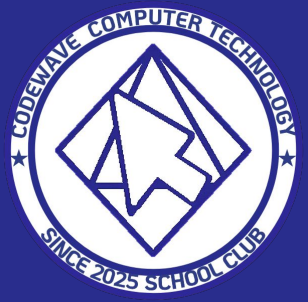
made by Yousol

정보보안 기초

동아리 필수 전공과목



정보보안이 무엇인가?

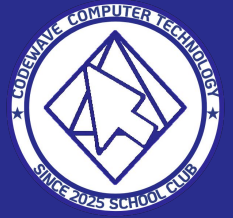
정보 보안이란 데이터의 **기밀성, 무결성, 가용성**을 보장하기 위해
다양한 방법과 기술을 사용하는 것을 의미합니다.

이 세 가지 원칙은 정보 보안의 가장 중요한 점이라고 할 수 있다고 보시면 됩니다.

기밀성

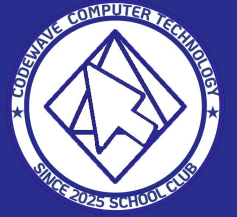
기밀성은 데이터를 **인가된 사용자**만 접근할 수 있도록 보호하는 것입니다.
민감한 정보가 무단으로 접근되거나 노출되지 않도록 하는 것을 목적으로 합니다.
예를 들어 **암호화**는 데이터의 기밀성을 유지하기 위한 대표적인 기술이라고 볼수 있죠?

무결성



무결성은 데이터가 무단으로 변경되거나 손상되지 않도록 **보장하는 것**입니다.
무결성을 유지하기 위해서는 데이터가 올바르게 저장되고 전송되는지를 확인하는
절차가 필요하다~

가용성



가용성은 인가된 사용자가 필요할 때 언제든지 **데이터에 접근**할 수 있도록 보장하는 것입니다.
이를 위해 네트워크와 시스템의 안정적인 운영이 필요하며, 공격에 대비한 대비책이 중요하다.

정보보안의 주요 위협

디지털 환경에서는 다양한 보안 위협이 존재합니다.

최근에도 SKT 정보 유출사고라는 큰 사건이 있었죠?
따라서 이번엔 보안의 주요 위협을 알아보겠습니다.

악성 소프트웨어(멀웨어) : 시스템을 손상시키거나
데이터를 훔치기 위해 설계된 소프트웨어이다.
대표적인 것이 바로 바이러스, 트로이 목마, 랜섬웨어이다.

피싱 : 사용자를 속여 개인정보를 훔치는 공격방식이다.

디도스(DDoS) : 다수의 컴퓨터가 동시에 특정 서버나 네트워크에 과도한 트래픽을 유발하여 서비스를 방해하는 공격이다.
예를 들어 유명 공연 티켓팅 할때 사이트가 들어가지지 않는것이..

정보보안의 주요 원칙

정보 보안을 강화하기 위해 개인과 기업 모두가 따라야 할 몇 가지 기본 원칙이 있습니다. 이러한 원칙은 데이터를 안전하게 보호하는 데 중요한 역할을 합니다~

강력한 비밀번호 사용 : 강력한 비밀번호는 해킹을 방지하는 첫 번째 방어선이다. 비밀번호는 보통 문자 , 숫자, 특수 문자를 조합해서 만드는게 좋고 주기적으로 변경해주는 것이 좋습니다~

이중 인증 : 로그인 시 추가적인 인증 수단을 요구하여 보안을 강화하는 방법이다. 귀찮더라도 이거 하면 해킹 시도는 보통 여기서 막혀요 (경험담)

보안 취약점

보안 취약점은 공격자가 시스템의 정보보증을 낮추는 데 사용되는 약점입니다.

쉽게 말해서 그냥 상대의 빈틈을 노린다~ 라고 생각하면 됩니다.
보안 취약점은 세 가지 요소를 갖추고 있는데

첫번째로 시스템에 결함이 있고
두번째로 공격자가 결함에 접근할 수 있으며
세번째로 공격자가 해당 결함을 익스플로잇(취약점을 이용한 공격)할 가능성이 있어야 한다.

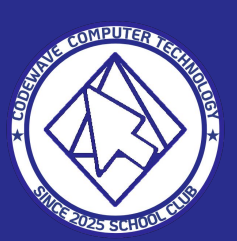
라는 요소가 있습니다.

그렇다면 이 취약점을 공격하는걸 우리는 뭐라고 해요?
해킹이라고 합니다.

화이트 해커

취약점(빈틈)을 찾아서 그 부분을 보호해주는 역할을 누가 할까요?
바로 우리가 '화이트 해커'라고 부르는 보안 분야 전문가가 하고 있습니다.

이러한 보안 분야에는 다양한 진로가 있습니다.
-기업 망 보안 담당자(대기업, 정부기관, 금융기관 등)
-제품 보안 담당자
-보안컨설턴트
-디지털 포렌식 전문가 등



정보 수집

1.정찰 : ex) 구글에 대한 각종 정보를 수집, 구글이 어떤 서비스를 하는지, IP주소가 무엇인지 등등 알아냄. (cmd)

2.스캐닝 및 취약점 분석 : 서버의 운영체제가 무엇인지 웹 서버 프로그램의 버전이 무엇인지 등 알아냄. 또한 어떤 취약점이 있는지 알아냄. (burp suite)

공격

3.침투 : ex) 정보수집 단계에서 어떤 사용자의 비밀번호를 알아내는 등 취약점을 이용하여 실제로 시스템으로 침투하는 단계.

포스트 익스플로잇

4.권한상승 : 침투했지만, 일반사용자의 권한밖에 얻지 못했기 때문에 시스템 전체에 접근할 수 있는 관리자권한을 획득하는 단계

5.백도어 관리 : 언제든지 해당 시스템에 접근할 수 있도록 만드는 단계.
주로 사용자를 추가하거나 백도어를 설치해서 관리.

6.흔적지우기 : 시스템 관리자가 해킹했는 것을 알아차리지 못하게 하고 추적또한 못하게 하는 단계

이러한 단계를 알아보는 이유는 해킹을 방지하는 과정에서도 중요한 역할을 하기 때문입니다~

취약점 찾기 실습