2024308기 김태현

보안 위협 모델링

STRIDE 기법 (by MS)

Spoofing Identity 다른 사용자인척 하는 것
= 계정도용

Tampering With Data 무결성 훼손
= 데이터 변조

Repudiation 행위 부인 가능성
= 로그 기록

Information Disclosure 정보의 유출
= 평문전송

Denial of Service (DoS) 시스템 자원고갈로
서비스 거부유도

Elevation of Privilege 일반 사용자의 권한 상승

S 미인증 상태로 세션에 정상적인 것처럼 침투할 수 있다.
↳ 물리적으로 가능한, 비정상적인 통신 감지로 2차 보안

T 전송중 유효하지 않은 데이터를 전송할 수 있다.
↳ 데이터를 암호화하고, 시드나 오류검증코드를 도입하여 전송하도록 한다.

R 비정상적인 이슈가 발생하면 즉시 알아차려야 한다.
"증거가 아니더라도 바로 내부 내에"
↳ 네트워크를 통해 송신되는 모든 행위를 별도의 서버에 기록(로깅)하도록 한다.

이슈는 알림발송

I 네트워크와 저장되는 모든 정보는 평문이 되도록 V

↳ 모든 데이터는 암호화하여 아니어야 한다.

보관하고 송수신해야 한다.

절대로 일반적인 방법으로 데이터를

조회할 수 없도록 해야 한다.

D 비정상적인 패킷이 그대로 들어오면을

↳ 비정상적인 패킷은 우회시키고 안된다.

프록시를 적용하여 서버침입을

최소화해야한다.

(도메인 연결 등을 프록시 적용
CX) 클라우드 플레어)

E 보안용량 고려을

└ 필요한 권한을 부여하지 않는다.

↳ 꼭 필요한 권한만 부여하도록 하고,

, 사용자에게 일반적으로

쉽게 권한조정이

안되도록 제한