사이버 보안의 종류 5가지

1. 네트워크 보안 : 허가되지 않은 액세스와 피해로부터 회사의 네트워크를 보호하기 위해 설계된 일련의 전략, 프로세스, 기술을 말한다. 네트워크의 요소에는 데이터 액세스, 데이터 가용성, 데이터 기밀성, 데이터 무결성이 있다.
2. 애플리케이션 보안 : 무단 액세스 및 수정과 같은 보안 취약점에 대한 위협을 방지하기 위해 보안 기능을 개발하여 애플리케이션을 추가하고 테스트하는 과정이다. 애플리케이션 보안 유형에는 인증, 권한부여, 암호화, 로깅 및 애플리케이션 보안 테스트, 개발자의 애플리케이션 코딩이 있다.
3. 정보 보안 : 컴퓨터 및 네트워크로의 확대, 발전하는 정보환경에서 모든 정보자원 하드웨어, 소프트웨어, 데이터 등을 위/변조, 유츌, 훼손 등과 같은 정보보안 사고로부터 보호함으로써 무결성, 기밀성, 가용성을 제공하는 것을 의미한다. 정보 보안을 위협하는 요소는 해커, 감염된 컴퓨터 및 소프트웨어, 정보 손실 및 파괴, 정보의 조작, 서비스 거부 공격, 정보의 노출이 해당한다.
4. 운영보안 : 비즈니스 환경이 계획되고 검증된 일정 수준으로 보호하기 위한 일련의 조치와 통제가 수행되는 것을 의미한다. 운영 보안의 요서로는 위협, 취약성, 자산이 있다. 운영 보안의 상대는 내외부 침입자와 부적절한 자원에 근접하는 사용자 및 운영자, 그리고 운영 환경에 대한 위협으로 볼 수 있다.
5. 재해 복구 : 각종 재해 및 위험요소에 의한 정보시스템이 중단됐을 때 이를 정산적으로 회복시키는 것을 의미한다. IT에서의 재해는 사전적 의미를 벗어나 지진, 태풍 등의 자연재해 및 전쟁, 해킹, 사용자의 실수 같은 내외부적인 요인에 의한 장애, 그리고 시스템 결함, 기계적 오류, 관리정책 오류 등 다양한 사례를 포함한다.