사이버보안 종류

1. 네트워크 보안

허가되지 않은 액세스와 피해로부터 기업의 네트워크를 침입하는 것을 보호하는 일련의 전략,프로세스,기술 등의 활동을 말한다.

네트워크 보안의 방법으로는

최신 소프트웨어를 유지, 사용자의 권한 관리, 신뢰할 수 있는 도구 사용, 데이터 백업,보안 정책 수립, 사용자 교육등의 방법이 있다.

2. 애플리케이션 보안

다양한 네트워크에서 사용되고 클라우드와 연결되므로 보안 위협과 침해 가능성이 많기 때문에

무단 액세스 및 수정과 같은 보안 취약점에 대한 위협을 방지하기 위해 애플리케이션 보안 기능을 개발,수정하고 테스트 하는 과정을 말한다.

앱을 더 안전하게 만드는 보안 활동이다.

애플리케이션 보안의 방법으로는

사용자 인증, 권한 부여, 암호화, 로깅 및 보안테스트, 개발자의 코딩 등의 방법이 있다.

3. 정보 보안

데이터 보안으로도 부르며 저장 상태나 머신 간 전송 상태에서 승인되지 않은 액세스나 조작으로부터 데이터를 계속 안전하게 유지하는 활동

데이터 보안의 방법으로는

중요한 데이터를 파악해서 항상 암호화된 상태를 유지하며, 최소한의 필수 데이터만 저장, 사용기간이 끝나면 폐기처분한다.

특수(관리자) 계정 정리로 최소한의 권한으로 업무 처리, 엄격한 내부 보안 경계선을 규정한다

4. 운영 보안

비즈니스 환경이 계획 검증된 일정 수준으로 보호되기 위한 조치 밑 통제행위로 영리한 악의적 행위자가 적절히 분석을 하거나

다른 데이터와 결합하는 방법으로 OPSEC이라는 약자로 표시되는 경우가 많다.

요소로는 위협, 취약성, 자산이 있다.

5. 재해 복구

각종 재해 및 사이버 공격의 위험요소에 의해서 정보시스템의 중단이나 데이터 손실이 발생했을때 상태를 바로잡아 복구하는 것을 말한다.

재해복구의 요소 및 절차에는 복구 제도 마련, 복구 조직 구성, 복구 시스템 구축, 복구 계획 및 절차 수립, 데이터 백업, 백업 관리, 복구 테스트, 사후 점검 및 확인이 있다