**사이버 보안의 종류 5가지에 대하여 나열하고, 그에 대하여 간략하게 서술하시오.**

사이버 보안의 종류 5가지는 네트워크 보안, 애플리케이션 보안, 데이터 보안(정보 보안), 운영 보안, 재해 복구가 있다.

네트워크 보안은 허가되지 않은 액세스와 피해로부터 회사의 네트워크를 보호하기 위해 설계된 일련의 전략, 프로세스, 기술을 말한다. 네트워크 보안의 데이터 요소는 데이터 액세스, 데이터 가용성, 데이터 기밀성, 데이터 무결성이 있다. 클라우드 보안은 클라우드에 저장된 데이터에 대한 데이터 개인정보 보호와 보안 및 규정 준수를 보장하는 것을 말한다. 네트워크 보안 모범 사례는 소프트웨어를 유지 보수, 가시성 최우선, 사용자의 권한 관리, 신뢰할 수 있는 도구 사용, 규정 준수 유지, 보안 정책 수립, 데이터 백업, 타사 사용자의 인지, 사용자 교육 등 9가지가 있다.

애플리케이션 보안은 무단 액세스 및 수정과 같은 보안 취약점에 대한 위협을 방지하기 위해 보안 기능을 개발하여 애플리케이션에 추가하고 테스트하는 과정이다. 애플리케이션 보안 유형은 인증, 권한 부여, 암호화, 로깅 및 애플리케이션 보안 테스트, 개발자의 애플리케이션 코딩이 있다. 애플리케이션 보안 제어는 코딩 수준에서 애플리케이션 보안 수준을 향상하여 위협에 대한 취약점을 줄이는 기술이다. 애플리케이션 보안 테스트 유형인 퍼징(fuzzing)은 일반적으로 비정상적인 데이터를 애플리케이션에 전달하여 에러를 유도하는 방법이다. 애플리케이션 개발자는 소프트 웨어 개발 프로세스의 일환으로 애플리케이션 보안 테스트를 수행하여 소프트웨어 애플리케이션의 새로운 버전 또는 업데이트된 버전에 보안 취약점이 없는지 확인해야 한다. 애플리케이션 보안 솔루션은 시큐어 코딩, 웹서버 악성코드 탐지, 웹해킹차단 시스템, 데이터 보안이 있다.

데이터 보안은 정보 보안(Information security)이라고도 한다. 정보 보안은 컴퓨터 및 네트워크로 확대, 발전하는 정보환경에서 모든 정보자원 하드웨어, 소프트웨어, 데이터 등을 위 · 변조, 유출, 훼손 등과 같은 정보보안 사고로부터 보호함으로써 무결성, 기밀성, 가용성을 제공하는 것을 의미한다. 정보 보안 위협은 해커, 감염된 컴퓨터 및 소프트웨어, 정보 손실 및 파괴, 정보의 조작, 서비스 거부 공격, 정보의 노출이 해당한다. 데이터 보안 강화 방법은 중요한 데이터 파악, 크리덴셜 정리, 엄격한 내부 보안 경계선 규정, 데이터 암호화 상태 유지, 클라이언트 보호 등이 있다. 클라우드 사용에 따른 데이터 보안 위협이 생기고 있다. 조직의 인프라가 디지털화 될수록 데이터 유출 사고를 겪을 가능성이 높아지는데, 디지털 트랜스포메이션을 이행하는 조직들이 경쟁 우위를 선점하고 있어, 기업들이 빠르게 혁신 기술을 도입하고 있으며 이로 인해 전에는 발생하지 않았던 데이터 유출 사고 및 데이터 규제 위반 사례가 나타나고 있다. 민감 데이터를 보호하기 위해서는 민감 데이터의 위치를 인지하는 것으로, 분류된 데이터는 강력한 멀티 클라우드 키 관리 전략으로 암호화 및 보호되어야 한다.

운영 보안은 비즈니스 환경이 계획되고 검증된 일정 수준으로 보호되지 위한 일련의 조치와 통제가 수행되는 것을 말한다. 운영 보안 요소에는 위협, 취약성, 자산이 있다. 운영 보안 상대는 내외부의 침입자와 부적절한 자원에 접근하는 사용자 및 운영자, 그리고 운영 환경에 대한 위협으로 볼 수 있다. 통제란 위험을 감소시키기 위하여 만들어진 정책, 절차, 업무, 조직 구조 등을 의미한다. 통제의 목적은 첫째, 조직의 경영 목적 달성 둘째, 위험이 적절히 예방되거나 적발 또는 수정될 것이라는 합리적인 확신을 제공하는 것이 있으며 셋째, 경영진이 제기한 관심사를 기반으로 하는 것에 그 목적이 있다. 통제의 종류에는 통제 적용 시점에 따라 예방 통제, 탐지 통제, 교정 통제가 있다. 그리고 저지 통제, 응용 통제, 트랜잭션 통제, 관리 통제, 운영 통제가 있다. 감사는 IS운영 전략이 조직의 운영 전략과 일치함을 보증하는 역할을 한다. IS감사 대상은 백업 통제, 프로세스 통제, 데이터센터 보안, 비상 계획, 시스템 도입 및 개발 표준, 라이브러리 운영 절차가 있다. 모니터링은 IS 설비에 영향을 미칠 수 있는 보안 사건을 식별하는 메커니즘과 도구, 기술을 포함한 개념으로 문제 식별과 해결에 그 목적을 두고 있다. 모니터링을 위한 기술로는 침입 방지, 침투 테스트, 클리핑 레벨 설정을 통한 위반 분석이 있다. 운영 보안의 위협은 자산의 손실을 발생시키는 원인이나 행위를 의미하며, 고의적이거나 우발적인 사건으로 발생 시에 시스템의 손상을 일으켜 기밀성, 가용성, 무결성에 손상을 가져올 수 있다. 위협은 우발적 실수, 부적절한 행위, 의도적 공격이 포함된다. 운영 보안의 취약성은 위협이 이용 가능한 시스템 상의 약점을 의미하며, 트래픽 분석을 통한 노출, 유지보수계정, 부팅이나 재부팅 등 IPL 취약성, Network address hijacking 이 있다.

재해 복구는 각종 재해 및 위험요소에 의해 정보시스템이 중단됐을 때 이를 정상으로 회복시키는 것을 의미한다. IT에서의 재해는 사전적 의미를 벗어나 지진, 태풍 등의 자연 재해 및 전쟁, 해킹, 사용자 실수 같은 내외부적 요인에 의한 장애, 그리고 시스템 결한, 기계적 오류, 관리정책 오류 등이 있다. 백업은 데이터 복구의 핵심 구성 요소로 데이터의 특성 시점 복사본을 만드는 것을 말한다. 백업 데이터는 구조적/비구조적 데이터 모두일 수 있다. 재해복구 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. 재해 복구 계획 수립을 위해 필요한 사항은 총 9가지이다. 내부 시스템 감사, 외부 공급 업체 확인, 취약점 이해, 카탈로그 시스템 및 서비스, 위험 경감, 재해 복구계획 문서화, 직원교육, 재해복구계획 테스트, 업데이트가 있다. 재해 복구 시스템 유형은 구축 형태별, 운영 주체별, 복구 수준별로 나눌 수 있다. 구축 형태별로 구분하면 독자 구축, 공동 구축, 상호 구축이 있으며, 운영 주체별로는 자체 운영, 공동 운영, 위탁 운영이 해당된다. 또한 복구 수준별로 보면 미러 사이트, 핫 사이트, 웜 사이트, 콜드 사이트가 있다. 재해 복구 시스템 구현기술로는 하드웨어적 복제 방식, 소프트웨어적 복제 방식, 데이터 전송 방식, 동기 복제, 비동기 복제가 있다. 재해 복구 시스템을 올바르게 구축하기 위해서는 일정 및 방안을 수립하고 재해 복구 및 체계를 구현한 후 테스트를 진행해야 한다. 마지막으로 운영 관리 및 완료 보고를 실시한다. 재해 복구 시스템 구축시 복구시간 목표와 복구시점목표를 고려해야 한다. 복구 시간 목표는 업무별로 서비스 중단을 감내할 수 있는 시간을 정의하는 것이다. 복구 시간 목표에 대한 정의가 완료되면 복구할 데이터 중요도 및 비용을 고려하여 복구 시점 목표를 정의해야 한다.