전사원이 알아야할 랜섬웨어와 악성코드 예방법

사이버 보안의 종류 1

1. 사이버 보안 종류의 개요

(1) 네트워크 보안 (2) 애플리케이션 보안 (3) 데이터 보안(정보 보안) (4) 운영 보안 (5) 재해 복구

2. 네트워크 보안

(1) 네트워크 보안이란? - 허가되지 않은 액세스와 피해로부터 회사의 네트워크를 보호하기 위해 설계된 일련의 전략, 프로세스, 기술을 말한다. (2) 네트워크 보안의 데이터 요소는? - 데이터 액세스, 데이터 가용성, 데이터 기밀성, 데이터 무결성 (3) 클라우드 - 클라우드 아키텍처 내에서 데이터와 정보를 보호하도록 설계된 기술 및 모범 사례를 포함하는 포괄적인 용어로 클라우드 보안은 클라우드에 저장된 데이터에 대한 데이터 개인정보 보호와 보안 및 규정 준수를 보장하는 것을 말한다. (4) 네트워크 보안 모범 사례 9가지 - 소프트웨어를 유지 보수 - 가시성을 최우선 - 사용자의 권한 관리 - 신뢰할 수 있는 도구의 사용 - 규정 준수를 유지 - 보안 정책을 수립 - 데이터 백업 - 타사 사용자의 인지 - 사용자 교육

3. 애플리케이션 보안

(1) 애플리케이션 보안이란? - 무단 액세스 및 수정과 같은 보안 취약점에 대한 위협을 방지하기 위해 보안 기능을 개발하여 애플리케이션에 추가하고 테스트하는 과정 (2) 애플리케이션 보안 유형 - 인증, 권한 부여, 암호화, 로깅 및 애플리케이션 보안 테스트, 개발자의 애플리케이션을 코딩 (3) 애플리케이션 보안 제어 및 테스트 - 애플리케이션 보안 제어는 코딩 수준에서 애플리케이션 보안 수준을 향상하여 위협에 대한 취약점을 줄이는 기술 - 애플리케이션 보안 테스트 유형인 퍼징(fuzzing)은 일반적으로 비정상적인 데이터를 애플리케이션에 전달하여 에러를 유도하는 방법 - 애플리케이션 개발자는 소프트웨어 개발 프로세스의 일환으로 애플리케이션 보안 테스트를 수행하여 소프트웨어 애플리케이션의 새로운 버전 또는 업데이트된 버전에 보안 취약점이 없는지 확인 (4) 애플리케이션 보안 솔루션 - 시큐어 코딩 - 웹 스캐너 - 웹서버 악성코드 탐지 - 웹해킹차단시스템 - 데이터보안