전사원이 알아야 할 랜섬웨어와 악성코드 예방법 과제 레포트

박수예

사이버 보안이란 컴퓨터, 네트워크, 데이터를 악의적인 공격 즉, 사이버 공격으로부터 보호하는 전반적인 활동을 말한다. 사이버 공격의 대상은 단순히 개인 또는 기업에서 그치지 않고 공공기관, 더 나아가 국가 전체의 인프라까지 사이버 범죄의 표적이 될 수 있다. 이러한 사이버 공격의 양상은 빠른 속도로 급격하게 변하고 있는 추세이다. 이에 따라 사이버 보안이 중요하게 대두되고 있다.

사이버 보안의 종류에는 네트워크 보안, 애플리케이션 보안, 데이터 보안, 운영 보안, 재해 복구가 있다.

네트워크 보안은 허가되지 않은 접근이나 피해에 대비하기 위해 설계된 전략, 프로세스, 기술을 말하는 사이버 보안의 한 종류로, 쉽게 말하자면 허가되지 않은 상태에서 네트워크의 침입을 막거나 방지하는 것을 말한다.

애플리케이션 보안은 무단 액세스 및 수정과 같은 보안에 취약한 부분에 대한 위협을 방지하기 위해 보안의 기능을 개발하여 애플리케이션에 추가하고 테스트하는 과정으로, 다르게 표현하자면 보안에 있어서 취약점을 찾아 수정하는 과정을 통해 애플리케이션을 더욱 안전하게 만드는 보안활동을 말한다.

데이터 보안 또는 정보 보안은 확대되고 발전하는 정보환경에서 모든 정보자원들을 데이터 위조, 데이터 변조, 유출, 훼손과 같은 정보 보안 위험에서 보호함으로써 데이터의 무결성, 기밀성, 가용성을 제공하는 것을 말하며 저장 상태나 기기 간 전송 상태에서 승인되지 않은 접근이나 조작에서 데이터를 안전하게 유지하는 활동을 말한다.

운영 보안이란 비즈니스 환경이 계획되고 검증된 일정한 수준으로 보호되기 위한 조치와 통제가 수행되는 것을 말한다. 악의적 목적을 지닌 행위자가 숨겨야 할 어떠한 정보를 노출시킬 수 있는 공공 데이터를 평가하거나 보호하는 프로세스이다.

재해 복구는 각종 위험요소에 의해 정보시스템이 중단되었을 때 이를 정상으로 회복시키기 위한 활동을 말한다. 사이버 상에서의 재해는 사전적인 의미에서 벗어나 자연재해 및 전쟁, 해킹, 사용자의 실수와 같은 내외적인 요인에 의한 장애, 시스템의 결함, 기계의 오류, 관리 정책의 오류 등의 다양한 것들을 포함하는 개념이다. 이러한 재해의 복구에도 사이버 보안의 활동으로 분류되는 요소들이 있는데, 예를 들어 사이버 공격으로 발생된 데이터의 손실이나 서비스의 중지를 복구하는 것이 여기에 포함된다.

이렇듯, 광범위하게 이용되는 사이버 세상에서 나날이 발전되어가는 사이버 공격으로부터 소중한 자산인 데이터를 보호하기 위해 사이버 범죄를 사전에 방지하는 사이버 보안에 대해 익히고 실천하는 습관이 사이버 세상을 살아가는 우리 모두에게 필요하다.