**< 사이버 보안 종류 5가지 >**

1. **네트워크 보안(Network security)**은 승인되지 않은 상태에서 기업 네트워크를 침입하는 것을 막거나 방지하는 활동이다.

개념 상으로 네트워크 보안은 개별적인 디바이스에 중점을 두는 엔드포인트 보안을 보완한다. 네트워크 보안은 이들 엔드포인트 디바이스가 서로 간의 결합 조직 상에서 어떻게 인터랙션하는지에 중점을 둔다.

네트워크 보안은 물리적인 또는 소프트웨어 방어 도구를 이용해 기반 네트워크 인프라를 승인되지 않은 액세스나 오용, 오동작, 수정, 파괴, 부적절한 노출 등으로부터 보호하는 프로세스이다. 이를 통해 컴퓨터와 사용자, 그리고 프로그램이 승인된 핵심 기능을 안전한 환경에서 수행할 수 있도록 보안 플랫폼을 만든다.

네트워크 보안은 승인받지 않은 사람이나 프로그램이 네트워크와 네트워크에 연결된 디바이스에 액세스하는 것을 막는 데 사용하는 툴과 작업으로 구현된다. 본질적으로 해커는 네트워크를 통해 사용자의 컴퓨터에 접근하지 못하면 해킹도 할 수 없다.

1. **애플리케이션 보안(Application security)**은 애플리케이션 코드의 취약점을 찾아서 수정해 앱을 더 안전하게 만드는 보안 활동이다.

애플리케이션의 수명 주기 전체에서 애플리케이션을 위협으로부터 보호하는 것을 목표로 프로세스, 도구, 규칙을 제어하는 것입니다. 사이버 범죄는 조직적이고 전문적이며 데이터, 지적 재산 및 민감한 정보를 훔치기 위해 기업 애플리케이션에서 취약점을 찾아 악용하는 데 중점을 둡니다. 애플리케이션 보안을 통해 조직은 고객, 비즈니스 파트너 및 직원을 포함한 내외부 이해관계자가 사용하는 모든 종류의 애플리케이션(예: 레거시, 데스크톱, 웹, 모바일, 마이크로 서비스)을 보호할 수 있습니다.

1. **데이터 보안으로도 부르는 정보 보안(Information security)**은 저장 상태나 머신 간 전송 상태에서 승인되지 않은 액세스나 조작으로부터 데이터를 계속 안전하게 유지하는 활동이다.

**정보** 보안은 즉 **정보**의 기밀성, 무결성 및 가용성 및 **정보** 기술이 적절한 조처에 의해 보호되고 있는 상태를 말합니다. **IT** 보안 보다는 **정보** 보안이라는 **개념**이 보다 포괄적인 의미를 띄며, 따라서 점점 더 많이 활용되는 추세입니다.

정보에 대한 위협이란 허락되지 않은 접근, 수정, 노출, 훼손, 파괴 등이다. 정보위협의 주체는 외부의 해커가 될 수도 있고, 내부인이 될 수도 있다. 정보에 대한 위협은 나날이 늘어가고 있기 때문에 모든 위협을 나열할 수는 없으나, 전통적으로 다음의 세가지가 정보 보안의 주요한 목표이다. (때로는 정보 보안만이 아닌 보다 넓은 **보안**의 목표로 이야기되기도 한다.)

-기밀성

허락 되지 않은 사용자 또는 객체가 정보의 내용을 알 수 없도록 하는 것이다. 비밀 보장이라고 할 수도 있다. 원치 않는 정보의 공개를 막는다는 의미에서 프라이버시 보호와 밀접한 관계가 있다.

-무결성

허락 되지 않은 사용자 또는 객체가 정보를 함부로 수정할 수 없도록 하는 것이다. 다시 말하면, 수신자가 정보를 수신했을 때, 또는 보관돼 있던 정보를 꺼내 보았을 때 그 정보가 중간에 수정 또는 첨삭되지 않았음을 확인할 수 있도록 하는 것이다.

-가용성

허락된 사용자 또는 객체가 정보에 접근하려 하고자 할 때 이것이 방해받지 않도록 하는 것이다. 최근에 네트워크의 고도화로 대중에 많이 알려진 서비스거부공격이 이러한 가용성을 해치는 공격이다.

1. **OPSEC이라는 약자로 지칭되는 경우가 많은 운영 보안(Operational security)**은 영리한 악의적 행위자가 적절히 분석을 하거나 다른 데이터와 결합하는 방법으로 숨겨야 할 ‘큰 그림’을 노출시킬 수 있는 퍼블릭 데이터를 평가, 보호하는 프로세스이다.

미군에서 파생 된 용어이며 잠재적 인 적이나 위협, 임무의 기밀성 및 / 또는 운영 보안을 위험에 빠뜨릴 수있는 모든 종류의 중요 정보를 거부하는 데 사용되는 프로세스입니다. 최근 OPSEC는 민간 부문에서도 두드러지고 있습니다. OPSEC에 해당하는 것에는 소셜 미디어 사이트에서 활동과 습관을 모니터링하고 직원이 이메일이나 문자 메시지를 통해 로그인 자격 증명을 공유하지 못하도록하는 것이 포함됩니다.

OPSEC를 수행하는 것은 공격 및 방어 보안 전략뿐만 아니라 일상 생활에서도 매우 중요한 역할을합니다. OPSEC를 사용하는 가장 큰 이유 중 하나는 OPSEC의 결함을 밝히는 데 가장 널리 사용되는 공격 인 doxing을 사용하여 사이버 범죄자, 해커 및 정부로부터 사용자에 대한 민감한 정보를 공개 할 수있는 데이터를 확보하지 못하도록 방어하는 것입니다.

1. **재해 복구(disaster recovery)**에도 사이버보안 활동으로 분류될 수 있는 요소들이 있다. 예를 들어, 사이버 공격으로 초래된 광범위한 데이터 손실이나 서비스 중지 상태를 바로잡아 복구하는 기법이 여기에 해당된다.

재해 복구는 재해의 영향을 받지 않는 외부 위치에서 데이터 및 컴퓨터 처리 작업을 복제합니다. 자연 재해, 장비 고장, 사이버 공격으로 인해 서버가 다운되면 비즈니스는 데이터가 백업된 두 번째 위치에서 손실된 데이터를 복구해야 합니다. 가장 이상적인 경우는 조직이 컴퓨터 처리 작업을 원격 위치로 옮겨 운영을 계속하는 것입니다.

사이버 공격과 극단적인 기후 변화가 점점 더 자주 발생함에 따라 비즈니스 연속성을 위한 재해 복구 계획의 중요성도 커지고 있습니다. 재해의 잠재적 영향을 수량화하는 리스크 평가 및 비즈니스 영향 분석은 재해 복구 계획에 대한 경영진의 지원을 확보하는 데 효과적인 툴입니다.

적절한 재해 복구 계획을 마련하려면 비즈니스 연속성에 가장 중요한 시스템과 데이터 및 데이터 복구에 필수적인 단계를 적시한 문서화가 이루어져야 합니다. 계획에는 백업의 빈도를 명시하는 RPO(복구 시점 목표)와 재해 발생 후 허용 가능한 최대 다운타임을 정의하는 RTO(복구 시간 목표)가 포함되어야 합니다. 이러한 측정지표는 조직의 재해 복구 계획을 구성하는 IT 전략, 프로세스, 절차를 선택하는 기준이 되는 한계치를 설정합니다. 조직이 수용할 수 있는 다운타임의 양과 조직이 데이터를 백업하는 빈도에 맞게 조직의 재해 복구 전략을 수립할 수 있습니다. 마지막으로, 계획이 제대로 실행되는지 확인할 수 있도록 재해가 발생하기 전에 계획을 정기적으로 테스트하는 것이 중요합니다.