

록히드마틴의 사이버 킬 체인 6단계

1 단계 : 정찰

이 단계에는 공격자의 수동 정찰과 능동 정찰이 모두 포함됩니다. 취약한 대상을 식별하는 것이 단계의 가장 중요한 목표이며, 공격자는 대상에서 최대한 많은 데이터와 지식을 수집하려고 합니다. 이것은 사이버 공격을 시작하기 전의 준비 단계입니다.

2 단계 : 무기화

정찰 단계가 완료되면 공격자는 다음 단계인 무기화로 넘어갑니다. 이 단계에서 공격자는 대상에 대한 공격을 수행할 수 있는 최상의 도구 유형을 결정합니다. 이 결정은 정찰 단계의 결과를 기반으로 합니다. 공격자는 DDoS (Distributed Denial of Service) 공격, 봇넷 공격 또는 멀웨어와 같은 방법을 사용하여 보안패치등의 방어가 되지 않은 시스템을 공격 할 수 있습니다.

3 단계 : 전달

전달 단계는 공격자가 악의적인 페이로드를 통해 공격을 전달하는 것입니다. 이 페이로드는 피싱 전자 메일, 드라이브 별 다운로드 공격 또는 스피어 피싱과 같은 다양한 수단을 통해 제공 될 수 있습니다.

4 단계 : 착취

악용 단계에서 공격자는 자신의 공격을 수행하기 위해 발견된 취약점을 악용합니다. 대상 시스템이 일반적으로 손상되고 공격이 시스템에 침입합니다. 이 단계에서 공격자는 이미 발판을 마련했으며 다른 멀웨어를 설치하여 추가 침입을 시도 할 수 있습니다.

록히드마틴의 사이버 킬 체인 6단계

5 단계 : 설치

악용 단계 후 설치 단계에는 악성 소프트웨어가 설치되어 침해 된 시스템 내부에 증가하는 과정이 포함됩니다. 사용자는 감염된 전자 메일을 다른 사용자에게 보내는 등의 조치를 취하여 자신의 시스템에 멀웨어를 설치 및 확산시킬 수 있습니다. 위반은 영향을 받는 네트워크를 통해 증가 할 수 있습니다.

6 단계 : 명령 및 제어

이 단계에서 공격자는 모든 권한을 갖습니다. 성공적으로 진입하여 기업의 방어 수단을 위반한 후에는 악성 프로그램을 악의적인 목적으로 사용할 수 있는 공격자가 완전히 명령하고 제어 할 수 있습니다. 여기에는 기밀 정보, 암호, 전자 메일 또는 공격자가 찾는 기타 정보를 보내는 것이 포함될 수 있습니다.

4차 산업혁명, 5가지 특징

첫 번째 [융합 혁명]

사이버+현실, 사람+사물, 그 외 전혀 이질적인 요소들의 결합을 말합니다.

두 번째 [초지능성].

인공지능, 빅데이터, 로봇, 자율차 등의 활약입니다.

4차 산업혁명의 엔진인데 한국의 기술력은 떨어집니다.

세 번째 축은 [초연결성].

4차 혁명의 싹줄로 불리는 5G(세대)통신과 사물인터넷, VR(가상현실), AR(증강현실), 센서 등이 주역입니다.

네 번째 축은 [초신뢰성].

IT는 '인터넷서 정보를 주고받게하는 시스템'이라면,

블록체인(Block Chain)은 '인터넷서 신뢰를 주고받게하는 기술'입니다

다섯 번째 축은 [초생명성].

바이오테크놀로지(BT)와 나노테크놀로지(NT) 등이 주역.

BT는 유전정보(지놈)분석/ DNA 재조합/ 줄기세포/ 유전자 편집기술을 통해, 장수사회 등 초생명 사회를 만들어낼 전망입니다.