1. 사고 사례 간단 설명

테슬라
보안 업체 맥아피(McAfee)의 연구원들이 테슬라의 무인 자동차들 중 오래된 모델들을 속여 위험한 속도로 가속하게 하는 데 성공하는 사건이 있었다. 대단한 해킹 기술을 사용한 것도 아니었다. 그저 까만색 전기 테이프를 교통 표지판에 붙였을 뿐이었다. 35mph라는 속도 안내판을 85로 바꿨더니 테슬라의 자동차가 속도를 크게 높이더라는 게 이 사건의 요지다.

사실 이 실험으로 진짜 문제가 되었던 건 테슬라 차량에 탑재되어 있는 모빌아이(Mobileye) 제품, 아이큐3(EyeQ3)라는 장치였다. 다행히 전기 테이프로 속일 수 있었던 건 예전 버전이고, 새로운 버전들은 이런 정도의 공격에 당하지 않는 것으로 나타났다. 게다가 테슬라도 최신 모델에서는 모빌아이 제품들을 전혀 사용하지 않고 있다.

맥아피는 “이번 실험의 목적은 스마트카의 위험성을 알리는 것이 아니라, 무인 자동차가 세상에 돌아다니기 전까지 해결해야 할 과제가 엄청나게 많다는 것을 알리는 것”이라고 설명했다. “10~20년 정도의 시간이 지나면 누군가 스마트카들을 속이기 위해 이러한 장난을 실제로 할 가능성이 높다고 봅니다. 지금은 실험에 그쳤지만, 앞으로 이런 문제는 현실이 될 것이며, 따라서 누군가 생명을 잃기 시작할 것입니다.”

[출처: 보안뉴스(https://www.boannews.com/media/view.asp?idx=93908)]

※ 사례 선택 이유:
보안 이슈란 당연히 엄청난 기술을 사용한다고 생각하며 검색을 하다가 이 기사를 보고 흥미로움을 느껴 선택하게 되었다.

2. 사고 사례에서 보안 자산, 위협, 위험을 식별하기

- 보안 자산: 유형 자산(자동차), 무형 자산(소프트웨어: 모빌아이(Mobileye), 아이큐3(EyeQ3))
- 위협: 자율주행기능이 탑재된 자동차의 속도 조절 장치를 해킹하는 행위
- 위험: 자율주행기능이 탑재된 자동차의 속도 조절 장치의 해킹 가능성

3. 보안 목적, 보안 요구사항, 보안 조치를 제안하기

- 보안 목적: 무결성
- 보안 요구사항: 보안 자산(소프트웨어)의 기능향상 및 업그레이드
- 보안 조치: 속도 인식 프로그램의 기능향상