자유주의 정보 18-16

본 내용은 아래 (기사)를 요약 번역한 내용임

Paul Fredrick and David Inserra

, How Congress Can Help Protect U.S. Companies From Cyber Attack,

January 30, 2018

의회가 사이버 공격으로부터 미국 기업들을 보호하는 방법

미국에 가장 빠르게 증가하는 위협 중 하나는 사이버 공간의 영역 안에 있다.

버튼만 누르면 외국 해커들과 악의적인 정부들이 미국 회사들을 목표로 삼아 미국 경제에 강타를 날릴 수 있다.

이 문제를 해결할 필요성을 인식한 Sen. Orrin Hatch, R-Utah 상원 의원은 지난주 청문회에서 Kirstjen Nielsen 국토 안보부 장관에게 적극적인 사이버 방어 조치에 대해 몇가지 질문을 던졌다. 본질적으로, 적극적인 사이버 방어는 해커들에 대해 반격하려는 민간 주체자들의 노력이다.

이에 대해 Nielsen은 기업들이 적극적인 사이버 방어에 참여하는 것을 돕기 위해 민간 부문과 협력하고자 하는 국토 안보부의 의지를 확인했다.

과거 정권들이 이러한 종류의 방어를 지원하는 것을 탐탁치 않게 생각해 왔기 때문에, 이는 상당히 고무적이다.

최근 미국 기업들에 대한 명백한 사이버 공격에 뒤이어, 제한된 형태의 적극적인 방어가 합법화되는 것이 중요하다. 간단히 말해서, 정부가 혼자서 대처할 수 없을 정도의 미국 기업들에 대한 많은 공격들이 있었고 앞으로도 있을 것이다.

기업들이 적극적인 사이버 방어에 참여하도록 허용하는 것이 왜 이득이 되는지에 대한 두가지 이유가 있다.
첫째로, 자가 방어를 허용하는 것은 그 회사들을 희생자에서 목격자로 전환하는 것이다. 적극적인 방어 능력으로, 해킹을 당한 기업들은 해커들을 식별하기에 더 좋은 장비를 갖추게 되어, 당국이 이 상황을 좀 더 효과적으로 다룰 수 있게 될 것이다.

둘째로, 기업들이 해커들을 더 잘 식별할 수 있는 환경을 조성해주는 것은, 정부가 제한된 시간과 에너지를 가장 중대한 공격에 집중할 수 있게 할 것이다.

헤리티지 재단의 사이버 보안에 대한 보고서에 따르면 해커가 자신의 활동을 수행하게 하는 성가심(기술로 인해 해킹을 수행하는 경우)에서 신원을 확인하려는(해킹을 시도하는 기술)기법에 이르기까지 다양한 사이버 방어 활동이 있다.

미국 기업들에게 적극적인 사이버 방어 능력을 부여하는 것에 관해서는, 헤리티지 재단은 불편함과 귀인 기술(attribution technique)에만 국한하는 것을 권장한다.

현재로서는 연방 및 주 차원의 법률로 인해 기업들이 국내 해커들에 대해 적극적인 사이버 방어를 수행할 수 없게 돼있다.

이를 변경하기 위해서는 모든 연방 법이 "권한 없는 보호 컴퓨터"에 접근하는 것을 금지함으로써 1986년의 컴퓨터 사기와 남용 법을 개정해야 한다.

외국의 사이버 법도 미국 기업들이 미국 밖에서 활동하는 해커들에 대한 적극적인 방어 능력에 영향을 미친다.

이런 장애물을 넘는 것은 어려운 일이며, 정부는 조심스럽게 이 문제에 접근해야 한다. 이 과정을 시작하기 위해서, 미국은 동맹국들과 적극적인 방어에 대한 대화를 가능하게 해야 한다.

국토 안보부가 민간 부문과 이 문제를 해결하고자 하는 욕망은 사이버 보안 개선을 위한 임무의 중요한 부분이지만, 궁극적으로는 의회 조치가 필요하다. 조지아 주의 Tom Grave 조지아 주 하원 의원의 '능동적 사이버 방어 원칙'은 올바른 방향으로 가는 한 걸음이다.

사이버 위협은 사라지지 않고, 그 강도와 양만 더 늘어날 것이다. 미국 기업들이 적극적인 방어로 그 위협과 싸울 수 있게 하는 것이 필요하다.

번역: 이희망

출처: https://www.heritage.org/technology/commentary/how-congress-can-help-protect-us-companies-cyber-attack