



2016년 사이버 보안 위협 전망과 미국의 보험 입법 동향

김진억 수석담당역

■ McAfee 연구소가 발간한 2016년 전망되는 사이버 보안 위협 활동에 관한 보고서¹⁾에 따르면 사이버 범죄의 수법이 보다 지능화, 기업화되고 사이버 범죄 대상도 웨어러블 기기, 종업원 홈시스템, 클라우드 서비스, 인터넷 연결 자동차, 금융정보 등으로 확장될 것으로 보임.

- 첫 번째, 2015년 모든 유형의 하드웨어와 펌웨어를 직접 공격하는 방식이 큰 화제를 불러일으키면서 2016년에도 이러한 공격이 지속될 전망이다.
- 두 번째, 랜섬웨어(Ransomware)²⁾ 공격도 증가될 것으로 보는데 이는 2015년에 수많은 초보 사이버 범죄자들이 랜섬웨어를 만들 수 있는 제작도구(Ransomware-as-a-service)를 이용하면서 범죄수익금도 나눠 갖는 범죄 비즈니스모델이 구축되었기 때문이다.
- 세 번째, 웨어러블 기기(Wearables) 대상 공격 증가가 예상되는데 웨어러블 기기에는 개인정보가 적게 저장되지만 이를 조정하는 스마트폰을 손상시킬 수 있어 피싱 공격 목표가 되고 있음.
- 네 번째, 종업원 홈시스템을 통한 우회공격이 증가될 것으로 보는데, 이는 기업이 기업 자체의 사이버 보안 수준을 지속적으로 높임에 따라 사이버 범죄자들이 기업 네트워크에 접근할 수 있는 종업원의 홈시스템을 통한 우회공격을 증가시키고 있기 때문이다.
- 다섯 번째, 기업의 클라우드 서비스이용이 보편화됨에 따라 보안수준이 낮은 클라우드 서비스에 대한 공격을 통해 우회 공격 활동이 증가될 것임.
- 여섯 번째, 인터넷 연결 자동차³⁾에 대한 공격 증가가 예상되고 있으며, 2016년까지 자동차의 12%가 인터넷으로 연결될 것으로 전망되지만 이에 상응하는 보안 체계는 아직 미비한 실정임.
- 일곱 번째, 개인을 식별할 수 있는 도난자료가 웨어하우스, 즉 일종의 블랙마켓에서 사이버 범죄자들에게 가치있는 정보 형태로 결합되는 추세가 증가됨.
- 여덟 번째, 금융정보 탈취 보안 위협 증가(무결성 공격, data integrity attack)⁴⁾가 예상되는데,

1) McAfee Labs(2015, 11), "Threat Predictions Report".

2) 랜섬웨어(ransomware) 몸값을 뜻하는 랜섬(ransom)과 재품을 의미하는 웨어(ware)의 합성어로, 사용자의 파일에 악성코드를 심어 감염시킨 후 삭제를 빌미로 금전을 갈취하는 위협에 이용되는 일종의 악성코드임.

3) 커넥티드 자동차(connected car)란 자동차와 IT 기술을 융합하여 상시 인터넷 접속이 가능한 자동차를 말함.

4) 무결성 공격은 기업 시스템 및 데이터를 노출되지 않게 변경, 생성, 삭제함으로써 금전적 이익을 편취하는 행위를 말함.

2015년 금융정보 탈취 공격으로 100개 은행에서 특정 금융거래 변경으로 약 3억~10억 달러가 편취되는 사건이 발생했으며, 2016년에도 금융기관을 상대로 노출이 어려운 공격이 증가될 것으로 보임.

■ 한편 동 보고서는 과거 5년간의 전망과 실제 발생한 사이버 보안 위협 활동에 대한 경험을 바탕으로 향후 5년간 발생할 사이버 보안 위협 활동에 대해 분석함.

- 이에 따르면, 향후 몇 년간 기술적으로 하드웨어와 펌웨어를 직접 공격하는 추세가 지속적으로 증가하고, 추적이 어려운 공격기술도 더욱 발전할 것으로 보이며, 향후 사물인터넷(IoT)과 웨어러블 기기들도 보편화되면서 사이버 공격 대상도 확대될 것임.
- 또한 사이버범죄관련 산업의 발달로 사이버스피아가 기업화되면서 금융기관 정보 조작을 통해 금융시장을 교란시키는 범죄도 증가할 것임.
- 한편 개인의 디지털 정보가 양적으로 많아지면서 침해리스크도 증가하여 각국에서 새로운 사생활보호규정들이 제정되고 개인들이 디지털 정보를 기업과 공유하면서 보상을 받는 가치교환시장들이 생길 것임.

■ 한편 미국에서는 2015년을 “건강보험회사 데이터 유출의 해”로 거론할 만큼 보험회사에 대한 사이버 공격 사건이 많았으며, 주보험감독당국들은 전미보험감독관협의회(NAIC)를 중심으로 보험회사, 보험소비자와 협력하여 선제적으로 대응하고 있음.

- 2015년 한해 미국에서는 Anthem Inc., Premera Blue Cross 등 건강보험회사들에서 9천만 건 이상의 민감한 개인정보가 유출되면서 보험관련 사이버보안 법제 마련이 가속화되었음.
- NAIC는 사이버보안규제지침을 채택(2015. 4. 16)하였는데, 이는 사이버보안 침해로부터 소비자들을 보호하기 위해 보험회사, 설계사, 대리점 등에 데이터 보안 유지를 촉구하고, 주보험감독당국 간 통일된 기준마련을 통해 보험산업과 주보험규제당국 간 이해관계 조정을 목적으로 함.
- 주마다 다른 사이버보안 요건에 대해 통일된 보험회사 검사표준을 제정하기 위해 재무요건검사핸드북 개정안을 만듦(2015. 9).
- 또한 NAIC는 개인정보 침해 시 보험계약자, 보험수익자 등을 지원하기 위해, 사이버보안소비자권리법 제정 목적의 로드맵을 마련함(2015. 12. 17).
- 한편 사이버보험관련 정보를 수집하고 보험회사의 사이버 보험상품 개발을 지원하기 위해, 사이버보험을 판매하는 손해보험회사들이 제출해야할 사이버보안관련 부속보고서 양식을 만들고 있음.

(McAfee Labs, CIPR 등)