보안이슈, 안전한 보안을 위한 발걸음

20180494 경영학과 김지원

'빛에는 어둠이 따르는 법이다.'

기술이 발달하면서 우리에게 편리함을 주지만, 기술들이 되려 우리에게 독으로 다가올 수 있다. 기술과 보안 성능이 함께 발전함에 따라 해커들도 그에 발 맞춰 지능적으로 발전하고있다. 해커들은 가치가 있는 자산들을 공격하고, 필요한 정보를 캐내어 금전적 이득을 취하거나 악용한다. 보안전문가들은 해커들의 공격을 막고 정보를 안전하게 보호하는 것에 목적을 두며 힘쓰고 있다.

보안 사고의 원인과 최신 보안 사고

보안전문가들이 꼽은 보안 사고의 발생 원인으로는 1) IoT 기기의 취약성 2) 보안이 취약한 오픈소스 3) 보안 기초 부족에 따른 계정정보 유출 4) APT 공격과 제로 데이 공격과 같은 지능적이고 고도화된 공격 5) 기존 솔루션의 한계점 등이 제기됐다. 과거에는 개인정보 유출 사건에서 대부분 기업들의 책임이 인정되지 않았으며 개인정보관련 법률이 있음에도 불구하고 몇 건의 유출사고에서 모두 기업들이 승소했다, 법원은 이 같은 경우 개인정보 유출에 대한 정신적인 손해를 일부 인정했지만, 유출된 개인정보로 인한 추가적인 손해를 명확하게 입증하지 못하거나 기업이 법에서 규정한 수준의 보안대책을 마련하고 시행했다면 과실이 없다고 보았기 때문이다. 하지만 국내에서는 옥션 사건의 판결 이후 조금씩 변화가 생겼다. 우리나라의 행안부와 방통위가 관련법 고시를 '조치는 최소한의 기준'이라고 수정하여 단순한 조치만으로는 책임을 다했다 볼 수 없도록 한 것이다. 즉, 허들 모델에 따르면 첫번째 허들은 넘어도 두번째 허들은 못 넘을 수 있다는 판단을 내리기 시작했다고 말 할 수 있다. 현재의 보안사고는 과거와는 달리 단순히 기업의 개인정보만을 유출, 변조, 훼손하는 것에 그치지 않고 있으며 다양한 방법을 통해 개인정보가 유출되고 있다. 그럼 최근 보안사고에 대해 알아보자.

1. 온라인 화상 회의 플랫폼

현재, 신종 코로나 바이러스 감염 확산으로 대부분의 학생들이 비대면으로 수업을 진행하고있다. 그 중 ZOOM이나 WEBEX, SKYPE 등 여러 실시간 화상 플랫폼을 이용하고있다. 하지만, 화상회의 플랫폼 사용량이 국내외로 급격하게 늘면서, 보안사고가 끊임없이 발생하여 사용자들에게 주의가 요구된다. 지난 달 미국에서는 ZOOM을 이용한 수업을 하던 도중 포르노 영상이 갑자기 재생되는 사건이 발생했다. 해커가 회상회의에 무단 침입하고 화면 공유기능을 이용해서 음란영상을 업로드한 것이다. 연 이은 해커들의 공격에 'ZOOM 폭격'이라는 신조어가 등장하기도 했다. 뿐만 아니라, ZOOM의 개인정보처리도 문제가 되고있다. 아이폰으로 ZOOM에 접속하면 개인정보가 페이스북으로 전달된다. 페이스북을 이용하지 않더라도 스마트폰 정보와 줌 이용시간이 페이스북으로 전송된 것으로 나타났다. 최근 캐나다는 회의 메시지를 암호화 시키는데 사용하는 암호화키를 줌 측이 중국 북경에 있는 서버로 전송한다는 결과를 발표했으며 사용자들의 회의 세션과

사용현황 등을 전부 모니터링 할 수 있다고 주장했다. 또한, ZOOM 서버 해킹을 통해 사용자 계정과 암호가 다크웹에 유포되고, 개발자도 원인을 모르는 zero day 취약점 또한 유포되고있다. 이러한 문제점은 사용자가 암호를 변경하더라도 제로데이 취약점이 있다면 재발 가능성이 다분한 것이다.

추가적으로 6월 7일 기준, 시스코 사이버 보안 연구원은 ZOOM에서 공격자가 채팅 멤버나 개인의 시스템 원격 해킹을 통해 침투 가능하게 만드는 취약점 2개를 발견했다고 블로그에 포스팅했다. 이 두 취약점 모두 디렉터리 접근 취약점으로 취약한 줌 소프트웨어를 사용하는 시스템에 악성코드를 실행하기 위해 임의 파일을 쓰거나 심는데 악용될 수 있다. 현재 ZOOM은 이러한 위협에 방어할 수 있도록 패치를 한 상태이며 ZOOM측에서는 사용자들에게 최신 버전으로 업데이트하도록 권고하고 있다.

사고예방 노력은?

교육부는 온라인 개강을 한 학생들이 안전하게 온라인 수업에 참여할 수 있도록 특별 사이버 보안 관제를 가동했다. 한국교육학술정보원이 운영하는 교육부 사이버안전센터는 원격교육 관련 사이트의 보안 취약성을 긴급 점검하고 보안 강화 방안을 마련했다. 비정상적인 접근 등 사이버 공격을 모니터링하면서 즉시 대응할 수 있는 체계를 갖췄고, KISA에서는 Zoom 같은 화상회의 프로그램에 해킹이나 DDos 같은 사이버 공격이 시도되는지 관리하도록 계획했다. 또한, 교육부는 화상회의 프로그램을 쓰는 교사·학생들의 보안 의식을 강화하기 위한 사용자 지침서도 제작·배포했다. 법적으로는 원격수업을 고의로 방해할 때, 정보통신망 이용촉진 및 정보보호 등에 관한 법률 등으로 규제하고 있다고 경찰청에서 밝혔다. 또한, 이중인증, 회의 참가용 비밀번호 사용, 회의 참가자 대기실 사용, 디바이스 한 대에서만 이용을 통해 개인이 예방할 수 있다. 마지막으로는 화상회의의 완벽한 암호화를 확신하지 않고 안전하게 이용하는 것이 중요하다.

2. IOT서비스

사물인터넷은 다양한 형태와 성능이 다른 기기들이 다양한 방식으로 연결되어 있어 기기별로 맞춤형 디바이스 보안 기술이 필요하다. 사물인터넷 보안은 ICT 시스템 뿐만 아니라 현실 차원의 문제이며 보안 및 안전 이슈를 함께 고려해야한다.

1) 2016년 4월 여수에서 버스정보 안내시스템을 해킹하여 70분간 음란영상을 노출시켰다. 자가망이 아닌 저렴한 일반 임대망을 이용했기 때문에 해킹에 더 취약했던 것이다. 동영상을 중단시키기 위해 노력했지만, 원격제어기능까지 막히게 만들었다.

2) 공유기 악성 앱 감염 사례

공격자는 취약한 공유기 비밀번호를 악용하여, 대량 해킹으로 스마트폰 13,501대에 악성 앱을 감염시켰다. 이후, 탈취한 정보를 이용하여 포털사이트 계정 11,256개를 부정하게 생성했다.

3) N번방 운영자였던 와치맨이 IP카메라를 해킹해서 얻은 불법 촬영물을 음란물 사이트에 유포했던 것으로 알려지면서 IOT 스마트 홈 보안기술에 대한 위험성이 커지고 있다. 해커가 공격할 시 사생활 피해와 범죄 피해로 이어지기 때문이다. IP카메라를 사용하면 유/무선 인터넷과 연결되어 영상을 실시간으로 보내고 원격으로 모니터링 할 수 있다. 과거의 인세 캠 보안사고도 이와 같은 맥락이다. 인세 캠은 설치된 웹 캠 영상을 해킹해 카메라 관리인이나 촬영 당한 사람의 동의 없이 인터넷에 게시해왔었다. 2014년 등장한 이후에 2016년 방송통신위원회에서 접속을 차단했다. 하지만 현재도 해외 IP로 우회하여 접속할 수 있는 것으로 알려져 사람들에게 두려움을 주고 있다. 그 외에도 아래 그림과 같이 사고가 발생할 수 있다.

사물인터넷 분야별 보안 위협 시나리오

분야	주요 내용
스마트TV	스마트TV에 탑재된 카메라 해킹 → 사생활 영상 유출
스마트가전	로봇청소기 원격조종 애플리케이션 취약점 해킹 → 로봇청소기 탑재 카메라로 실시간 모니터링
공유기	수십만대 규모 공유기 해킹 → 악성코드 넣어 디도스 공격 창구 활용
스마트카	차량네트워크 침투 가능 조립 회로보드 → 브레이크 조작, 방향 설정, 경보장치 해제 등 가능
교통	도로차량 감지기술 내 광범위한 설계 및 보안 결함 발견 → 센서를 가장해 교통관리시스템에 위조 데이터 전송 가능
의료기기	인슐린 펌프 조작 → 치명적인 복용량 주입 가능

자료 : 한국과학기술기획평가원(KISTEP)

사고예방 노력은?

3)과 같은 보안사고를 예방하기 위해서 LH와 SH에서는 공공기관인 KISA의 IOT 보안인증서를 요구한다. 그리고 KISA는 건설사와 사물인터넷 제품 제조회사에서 서비스를 위해 구축한 IOT기기에서 발생할 수 있는 취약점을 사전에 점검하는 제도를 도입하고 홈네트워크 건물인증 보안점검도 운영하고 있다. KISA에서는 IOT 제품을 처음 사용할 시에 인증정보를 설정하고, 초기의 인증을 변경하는 것을 필수해야 한다고 정했다.

기관	보안 가이드
KISA	IoT 공통보안원칙, IoT 공통보안 가이드, 홈 · 가전 IoT 보안가이드
SK인포섹	사물인터넷(IoT) 보안 가이드라인
GSMA	서비스 생태계, 엔드 포인트 생태계, 네트워크 운영자를 위한 IoT 보안 가이드
OWASP	OWASP IoT Top 10

그 외에도 모든 IOT 제품의 최초 설계/개발부터 서비스 단계의 생명주기별 각 역할에 따라 보안 내재화와 설계단계에서 위 그림과 같은 IOT가이드라인 적용이 반드시 필요하다. IOT 서비스를 운영한다면, IOT디바이스를 포함하는 IOT 보안진단 프로세스를 구축하여 운영과 보안 취약점이 발생할 가능성에 대비해 업데이트 기능을 제공하여 신속하게 보안 패치가 이뤄지도록 하는 것도 중요하다. 개인에게는 패스워드 설정, 암호화 설정, 접근제어 설정 (IP/MAC 주소 인증), 펌웨어 업데이트 등을 통한 예방이 권고되어진다.

3. **인공지능**

1) 딥 페이크란 AI 기술을 이용해 특정인물의 영상, 사진, 목소리를 영상에 합성한 편집물이다. 이 기술이 발전하여 점점 더 식별하기 어렵다면 해커가 이 기술을 피싱에 악용할 가능성이 있으며 실제 특정 대상을 사칭하여 개인정보를 끄집어내고 이익을 취한 사건이 발생했다. 이 사건은 딥 페이크를 이용하여 해커들이 한 CEO 의 목소리를 똑같이 생성하여 2 만 달러를 송금하도록 속였다. 국내 금융기관에서도 비 대면 서비스를 제공할 때 실명확인을 위해 목소리, 얼굴 등을 이용한 바이오 인증을 접목하고 있어 딥 페이크 공격 발생 위험이 증가하고있다.

2) AI 스피커는 이제 우리 일상생활에서 쉽게 찾아볼 수 있다. 대화를 걸면 사용자의 음성명령을 인식하여 요구하는 기능을 수행하며, 점점 더 똑똑해 지고 있다. 날씨 안내, 음악 재생, 음식 배달, 등 편리한 기능을 수행하지만 이런 편의성 뒷면에는 개인정보 유출 및 해킹사고 발생에 대한 우려도 존재한다. AI 스피커는 음성 데이터를 중앙서버와 클라우드에 저장하여 이를 기반으로 기계학습을 시켜 정확도를 높이는 훈련을 하기 때문에 사용자의 음성데이터를 항상 듣고 있는 상태이며, 이를 계속적으로 서버에 전송한다. 이 때 중간에 해킹이 이뤄질 수 있고, 기기 자체를 해킹하여 데이터를 탈취할 수 있다. 2018 년 미국에서는 부부의 대화가 아마존 AI 스피커 에코를 통해 제 3 자에게 유출되는 사고가 발생했다. AI 스피커의 소리인식에 오류가 생겨 부부대화를 녹음하고, 그 파일을 연락처에 저장된 누군가에게 전송한 것이었다.

사고예방 노력은?

2019 년 4 월 8 일 유럽연합 집행위원회가 세계최초로 인공지능 윤리 가이드라인을 발표했다. 가이드 라인은 요약에서 "목적은 신뢰할 수 있는 인공지능을 알리는 것"이라며 신뢰할 수 있는 AI 에는 반드시 지켜져야 하는 세 가지 구성 요소에 대해 밝혔다. 이는 (1) 합법적이어야 하며 모든 관련 법규를 준수해야 한다. (2) 윤리적이어야 하며 윤리적 원칙과 가치를 준수해야한다. (3)좋은 의도로 AI 시스템이 의도하지 않은 결과를 초래할 수 있기 때문에 기술 및 사회적 관점 모두에서 견고해야 한다." 로 구성되어 있다.

3 개 장으로 구성된 가이드라인은 1 장에서 윤리적 원칙과 관련 가치를 언급했다. 중심내용이 포함된 2 장에서는 7 가지 핵심지침을 제시했다. 신뢰할 수 있는 AI 란 (1) 인적 기관 및 감독 (2) 기술적 견고성 및 안전성, (3) 개인 정보 및 데이터 거버넌스, (4) 투명성, (5) 다양성, 차별 금지 및

공정성, (6) 환경 및 사회복지 (7) 책임성을 갖춰야한다. 3 장은 작동 가능을 목표로 구체적이며 신뢰가능한 AI 평가 목록을 제공한다.

우리나라 정부의 경우 작년 10 월 28 일 대통령이 직접 발표한 '대통령 인공지능 기본구상'을 바탕으로, AI 강국으로 나아가기 위한 'AI 국가전략'을 발표했다. 해당 전략은 선택과 집중을 추구하는 동시에 AI 기술의 경쟁력 강화와 사람 중심의 AI 실현을 위한 추진과제들을 포함한다. 보안 부문에서는 AI 의 역기능과 보안 위협에 대비하고 안전한 AI 를 위한 윤리기준을 마련하는 내용과 AI 기반 사이버 위협 대응시스템 구축 및 정보취약계층 접근성 활용 역량 강화 내용이 포함됐다. AI 기술 활용과 확산에 따라 보안 위협 뿐만 아니라 딥 페이크와 같은 새로운 형태의 범죄도 출현하여 윤리문제에 대응하는 새로운 규범을 마련했다. 법안 현황으로는 3 월 5 일 국회 본회의에서 '성폭력 범죄의 처벌 등에 관한 특례법 일부개정안' (딥 페이크법)이 통과되었다. 법안은 인공지능 기술을 이용해 사람의 얼굴이나 신체 등을 합성/편집해 성적 욕망 또는 수치심을 유발할 수 있는 가짜 영상 등을 제작하면 5 년 이해 징역 또는 5000 만원 이하 벌금 등의 내용을 담고 있다. 개인은 인공지능 스피커를 사용할 때 기기의 주기적인 소프트웨어 업데이트, 보안강도가 높은 제품구매, 프라이버시 노출을 원하지 않을 때 전원을 끄거나 MUTE 버튼으로 사고 예방 가능하며, 딥 페이크 사고 예방을 위해 신뢰 가능한 사람이나 포탈에 자신의 정보를 올리는 것이 중요하다.

결론

기술이 발달할수록 보안이 가지는 중요성과 그 의미가 점점 더 커질 것이다. 보안 사고 예방과 사고발생의 피해를 최소화 하기 위해서는 정보보호 및 개인정보보호 관리체계 (ISMS-P)와 같은 정형화된 보안 관리 체계 수립과 실천이 기업 문화에 내재화 되어야한다. 또한, 사건을 예방할 수 있는 보안 정책은 국가 보안 경쟁력 강화와 같은 순기능을 극대화하는 정책과 양극화, 안전사고와 같은 역기능을 최소화 할 수 있는 정책 추진이 동시에 일어나야 한다고 생각한다. 현재 보안을 강화를 위해 많은 노력을 기울이고 있지만, 아직까지는 부족한 점이 많아 보이며 보안 규제 환경의 조성에 있어서도 혁신 촉진을 위한 규제의 정비와 함께 안전을 보장하는 규제 구축이 균형 있게 이뤄져야한다. 정보주체도 기업과 사회의 노력에 맞게 자신의 개인정보를 보호하기 위해 노력할 필요성이 대두된다. 짧게 보면 보안사고는 손실을 가져오겠지만, 이를 토대로 더욱 보안성이 강화된 제품을 만든다면 강화된 보안의 새로운 발걸음이 될 것이다.