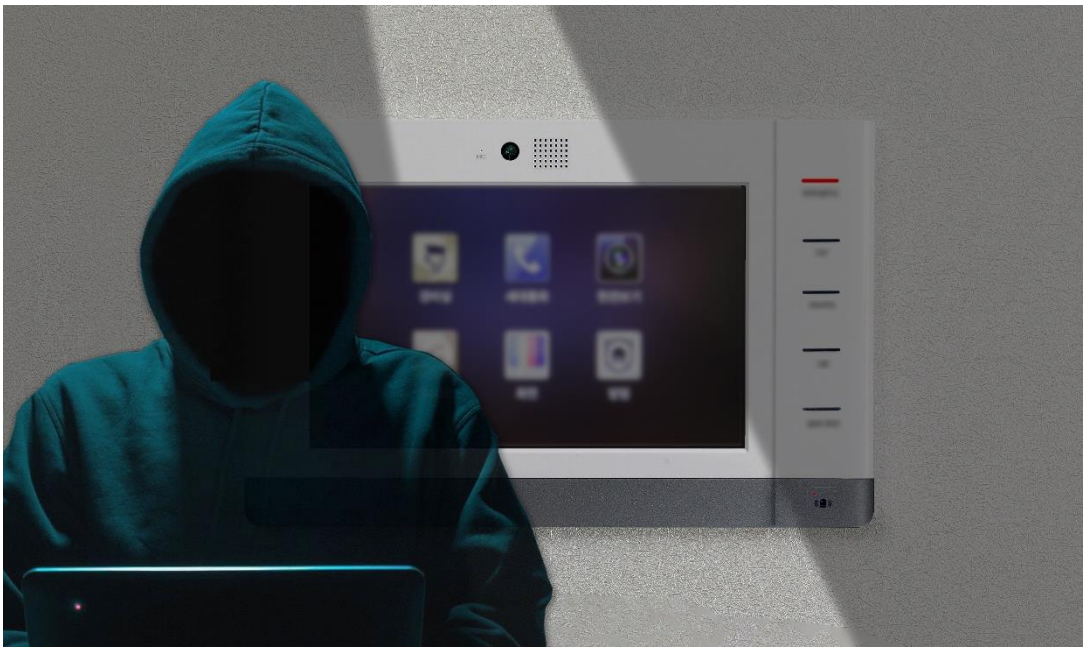
EQST insight

우리 집 스마트 홈 기기 월패드 안전할까?
월패드 보안 위협 분석과 대응 방안

최근 700여 곳에 이르는 국내 아파트의 월패드 카메라가 해킹되고, 사생활이 노출되는 사고가 잇따르고 있다. 이번 헤드라인에서는 월패드 보안 위협 분석과 대응 방안에 대해 설명하고자 한다. 월패드란 아파트·빌라 등 가정의 벽면에 부착된 단말기로 현관 출입문 통제, 가전제품 냉난방기와 환기시설 제어, 엘리베이터 호출 및 인터넷 접속, 세대 간의 화상 통화, TV 수신 등 다양한 부가기능을 갖춘 장치다. 또한 IoT 기술을 적용해 가정 내 스마트 기기를 연결 및 제어할 수 있다.



최근 월패드 해킹 이슈

월패드는 우리 생활을 편리하게 만들어주지만, 우리 생활의 안전 역시 위협하고 있다. 스마트 홈 기기는 네트워크에 연결되어 있어 외부에서 접근이 가능하다는 점이 가장 큰 원인이다. 스마트 홈 기기가 보편화된 만큼 이를 악용한 해커들의 공격이 급증하고 있다.

최근 발생한 월패드 해킹 사건은 월패드 내부 카메라의 영상을 탈취해 다크웹에서 고가의 금액으로 거래가 이루어져 큰 이슈가 되었다. 해당 아파트 입주민들은 월패드의 내부 카메라를 스티커로 막는 등 임시 대응을 하고 있지만 근본적인 대책 마련이 필요한 상황이다.

월패드 보안 위협 시나리오

아파트 네트워크 시스템은 다양한 네트워크 구조로 구축이 된다. 스마트 홈 기기를 관리하는 중앙관리서버가 존재하며, 월패드는 이 [1]중앙관리서버에 연결되어 운영되고 있다. 중앙관리서버는 외부의 접근으로부터 서버를 안전하게 보호하기 위해 [2]서버 OS 방화벽을 구축하거나 [3]UTM 과 같은 보안솔루션 도입하여 중앙관리서버에 쉽게 접근하지 못하도록 구성되어 있다.

만약 유지 비용, 운영 관리 등의 사유로 보안솔루션 도입이 불가능하거나, 서버 OS 방화벽이 기본 설정으로 되어있을 경우, 다음과 같은 월패드 보안 위협 시나리오가 발생할 수 있다.

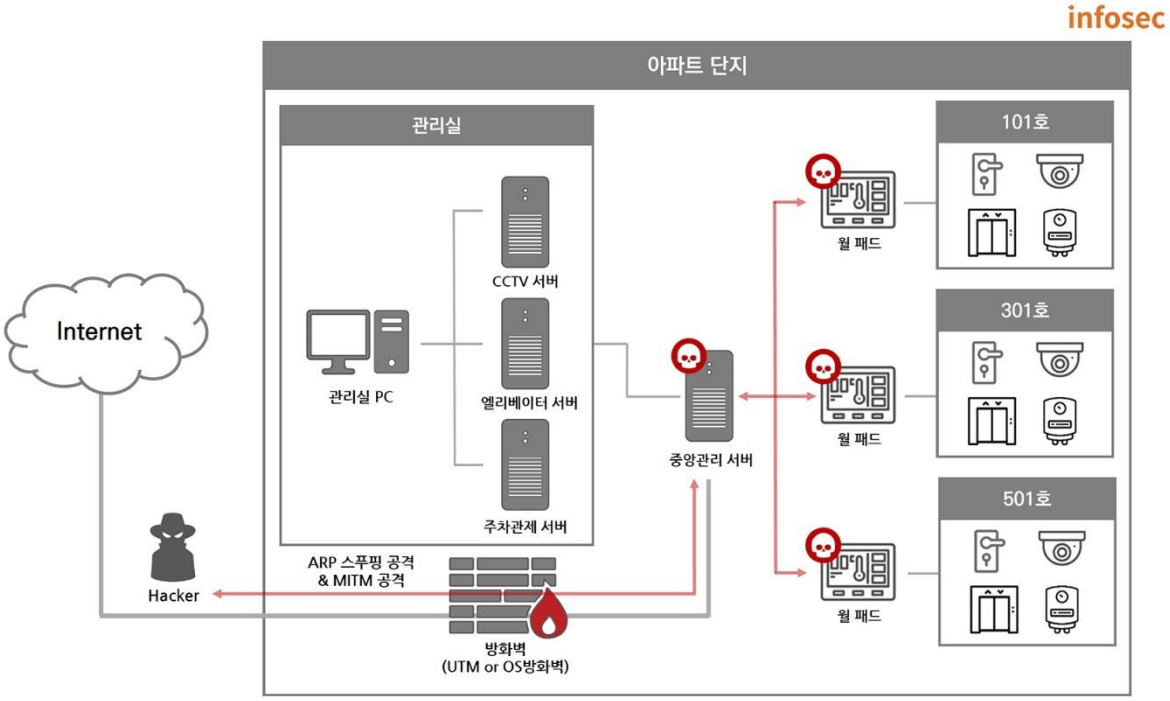
---

[1] 중앙관리서버 : 아파트 내 네트워크 기기들을 관리하기 위한 중앙관리서버

[2] 서버 OS 방화벽 : 서버에서 기본적으로 제공하는 방화벽기능

[3] UTM (Unified Threat Management) : 통합위협관리는 방화벽, VPN, IPS 등 다양한 보안 기능을 단일 어플라이언스 형태로 통합한 보안 솔루션을 말한다.

1. 중간자 공격(MITM)을 통한 접근

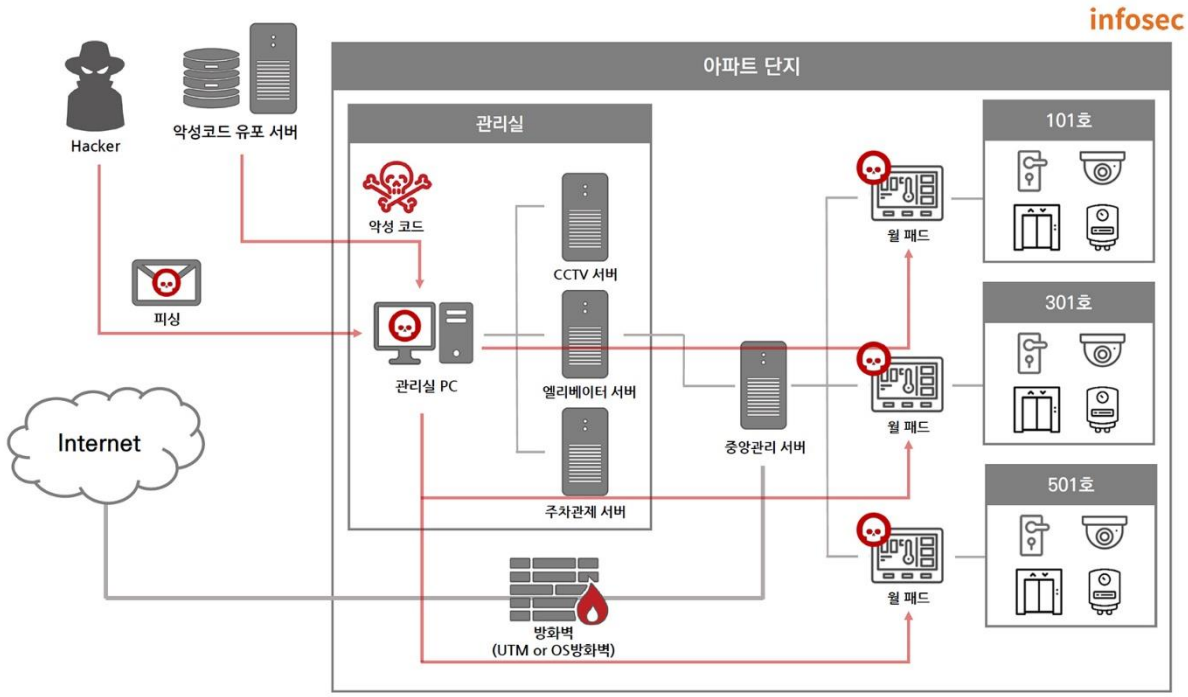


서버 OS 방화벽이 기본 설정으로 취약하게 구성되어 있을 경우, 해커는 [4]ARP 스푸핑 공격과 [5]MITM 공격을 이용하여 자신의 IP 주소가 방화벽 정책에 허용된 IP 주소인 것처럼 속여 방화벽을 우회해 중앙관리서버 접근할 수 있다. 중앙관리서버 접근 후 월패드 시스템까지 접근이 가능하고 이후 권한 획득을 통해 영상 탈취, 인증 정보 획득 등 2차 공격으로 이어질 수 있다.

[4] ARP 스푸핑 (Address Resolution Protocol Spoofing) : MAC 주소를 사용자의 컴퓨터가 아닌 다른 사용자의 컴퓨터 MAC 주소인 것처럼 조작하는 공격 유형

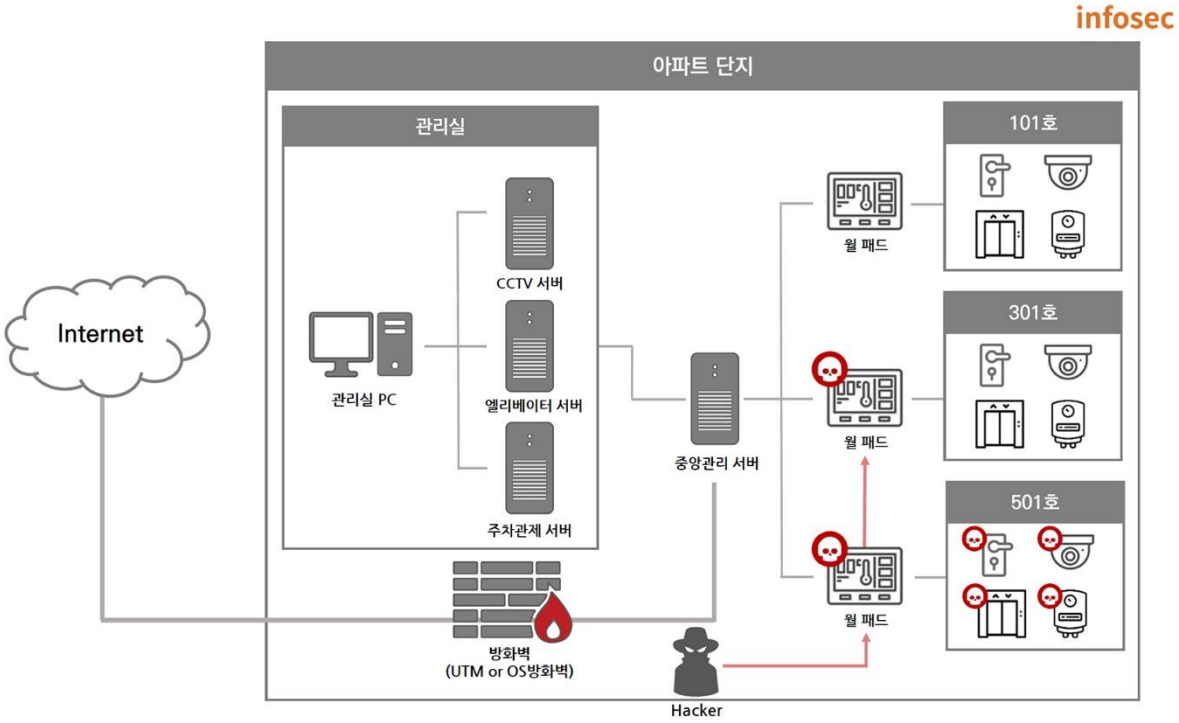
[5] MITM (Main in the middle attack): 중간자 공격. 악의적인 사용자가 네트워크에 침입하여 데이터 스트림을 수정하거나 거짓 생성하는 컴퓨터 보안 침입

2. 관리자 컴퓨터 PC 악성코드 감염을 통한 접근



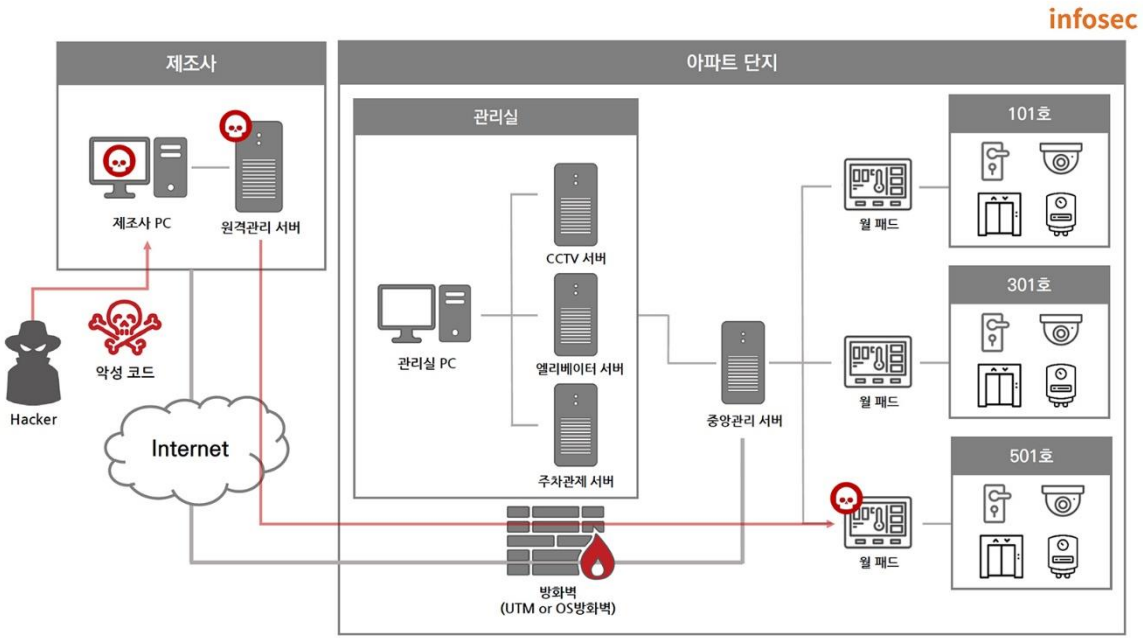
아파트 관리실 컴퓨터의 경우 월패드 관리를 위해 중앙관리서버에 접근이 가능하다. 해커가 관리실 컴퓨터를 대상으로 한 피싱 공격을 통해 악성코드를 설치할 경우, 관리자 컴퓨터 권한을 획득할 수 있다. 이후 내부 시스템 접근 및 중앙관리서버 서버 권한 획득을 통해 연결되어 있는 각 세대의 월패드 장악이 가능하다.

3. 원격제어 프로그램을 통한 접근



제조사에서 월패드에 대한 유지 보수를 위해 원격 프로그램을 사용하여 기능 버그 탐지 및 오류 점검을 진행한다. 원격 프로그램에서 사용하는 포트가 외부에 노출될 경우, 해커는 노출된 포트를 통해 월패드에 원격 접근이 가능하게 된다. 이후 월패드 권한 획득을 통해 2차 공격이 가능하다.

4. 공급망(제조사) 공격을 통한 접근



제조사에서는 월패드 펌웨어 업데이트를 위해 원격관리 서버가 존재하고 있다. 해커는 제조사에서 사용 중인 PC를 대상으로 피싱 등의 공격을 통해 악성코드를 감염시키고, 원격관리 서버에 침투해 펌웨어 업데이트 파일을 변조한다. 이후 가정에서 사용 중인 월패드에서 자동 업데이트 기능으로 변조된 펌웨어 파일이 설치될 경우 해커는 월패드 권한 획득이 가능하다. 동일한 방식으로 제조사를 통해 관리되는 모든 월패드에 공격이 가능하다.

5. 그 외 치명적인 해킹 위협 시나리오

현재까지는 해커가 월패드 카메라를 해킹해 촬영된 영상을 유출 및 다크웹에 거래하는 피해 사례가 발생했다. 하지만 월패드에는 카메라 기능만 있는 것이 아니라 집안의 온도 조절 및 가스나 전기 시스템 등 다양한 부가 기능이 연동되어 있다. 따라서 관련 기능에 공격이 이뤄질 경우 생명에 위협을 끼치는 테러 활동이 가능하며, 시스템이 도어락까지 연동되었을 경우 무단 주거 침입까지 발생할 수 있다.

월패드에 대한 보안 대응 방안

1. 이용자의 월패드 보안 수칙

월패드는 시스템 설정 변경 시 관리자와 사용자의 비밀번호가 필요하다. 관리자 비밀번호는 기본적인 비밀번호로 설정되어 있기 때문에 이를 변경하여 사용하도록 해야 한다. 제조사마다 비밀번호 변경 방식이 다르기 때문에 이를 확인하여 변경하도록 한다.

월패드의 내부 카메라를 사용하지 않은 경우 스티커 등을 통해 가리도록 한다. 또한, 주기적인 최신 업데이트를 통해 취약점이 제거된 안전한 버전을 사용할 수 있도록 한다.

2. 엔드포인트 보안 강화

과학기술정보통신부, 국토교통부, 산업통상자원부 등 3개 부처에서 월패드 망 분리 의무화 규정을 추진 중이다. 아파트 단지 서버와 세대별 홈게이트웨이 사이의 망은 물리적 방법으로 분리하거나, 소프트웨어를 활용한 VPN, VLAN, 암호화 기술 등을 활용해 논리적 방법으로 분리 구성해야 한다.

하지만 '망 분리만 적용되면 홈네트워크 보안 사고는 안전하다'라는 인식은 위험하다. 세대별로 망 분리를 하더라도 세대의 각 중앙 서버와 연결돼 있다. 옆집에서 옆집으로 감염되는 방식의 공격은 막을 수 있으나, 옆집에서 중앙 서버를 거쳐 전체 세대로 확산하는 것은 막기 힘들다.

폐쇄망을 구성한다고 하더라도 가정에서 인터넷을 사용하고 있기 때문에 효과가 제한적일 수 있다. 공유기를 타고 스마트폰, PC, 로봇청소기, 냉장고로 감염이 전파될 수 있다. 하나라도 홈네트워크에 연결되어 있다면 감염될 수 있다는 것인데, 폐쇄망을 쓰는 기업, 공공기관 등의 해킹 사례가 발생하는 것과 같다.

그러므로 엔드포인트에 대한 강화가 필요하다. 월패드에 대한 시스템 취약점을 제거하고 주기적인 보안 업데이트와 제조업체 원격 지원 서비스 시 VPN과 사용자 서명 인증 값을 이용하여 비인가자에 대한 접근을 제어할 수 있도록 해야 한다.

3. 스마트 홈 기기 제조 업체에 대한 보안 규제 강화

월패드 및 홈 네트워크 IoT 기기 제조업체들이 보안 요구사항을 고려한 제품을 개발하고 지속적으로 업데이트를 지원해야 한다. 법 제도 정비로 관리 책임에 대한 소재도 명확히 해야 한다. 이와 관련하여 과학기술정보통신부, 국토교통부 및 산업통산자원부는 사물인터넷(IoT) 융합기술발전 및 홈네트워크에서 발생할 수 있는 보안 위협을 예방하고자 '지능형 홈 네트워크 설비 설치 및 기술기준(이하 지능형 홈네트워크 고시')을 21년 12월 31일 개정했다. 아래 표는 이번에 개정된 고시 내용으로 22년 7월 1일부터 시행되며, 고시 시행 이후 주택건설 사업을 승인받아 시행하는 건설사들은 홈 네트워크 설비를 설치할 때 개정된 고시 내용을 준수해야 한다.

infosec

구분	보안 요구사항
데이터 기밀성	이용자 식별정보, 인증정보, 개인정보 등에 대해 암호 알고리즘, 암호키 생성·관리 등 암호화 기술과 민감한 데이터의 접근제어 관리기술 적용으로 기밀성을 구현
데이터 무결성	이용자 식별정보, 인증정보, 개인정보 등에 대해 해쉬함수, 전자서명 등 기술적용으로 위·변조 여부 확인 및 방지 조치
인증	사용자 확인을 위하여 전자서명, 아이디/비밀번호, 일회용비밀번호(OTP) 등을 통해 신원확인 및 인증 기능을 구현
접근통제	자산·사용자 식별, IP관리, 단말인증 등 기술을 적용하여 사용자 유형 분류, 접근권한 부여·제한 기능 구현을 통해 인가된 사용자 이외에 비인가된 접근을 통제
전송데이터 보안	승인된 홈네트워크장비 간에 전송되는 데이터가 유출 또는 탈취되거나 흐름의 전환 등이 발생하지 않도록 전송데이터 보안 기능을 구현

< 홈네트워크장비에 대한 보안 요구사항(제14조의2제2항 관련)(신설) >

과학기술정보통신부와 한국인터넷진흥원(이하 KISA)는 18년부터 사물인터넷(IoT) 보안 인증 서비스를 시행하고 있다. 이번에 제정된 고시의 경우도 KISA 수행하고 있는 IoT 보안 인증을 법제화한 것으로 확인된다. 인증기관은 KISA에서 진행하고 있으며, 시험 대행 기관은 한국정보통신기술협회(TTA)에서 진행하고 있다. 시험·인증 기준은 '홈네트워크 장비에 대한 보안 요구사항' 고시된 항목보다 상세한 항목으로 진행하고 있다.

infosec

인증영역	인증기준
식별 및 인증	안전한 인증정보 사용, 사용자 인증 및 권한 관리, 비인가 상호인증 제한, 반복된 인증시도 제한, 정보노출 방지, 안전한 세션관리
데이터 보호	전송·저장 데이터 보호, 중요정보 저장 영역 보호강화, 개인정보 법적 준거성, 중요정보 완전삭제
암호	안전한 암호 알고리즘 사용, 안전한 암호키 생성, 안전한 암호키 관리, 안전한 난수 생성
소프트웨어 보안	시큐어코딩, 소스코드 난독화, 소프트웨어 보안기능 시험, 알려진 취약점 조치, 불필요한 기능 및 코드 제거, 안전한 소프트웨어 적용, 감사기록
업데이트 및 기술지원	모델명 및 제품정보 확인, 안전한 업데이트 수행, 업데이트 파일의 안전성 보장, 업데이트 실패 시 복구, 업데이트 기술 지원, 업데이트 정보 제공, 자동업데이트 기능 제공
운영체제 및 네트워크 보안	안전한 운영체제 적용, 불필요한 계정·서비스·포트 통제, 불필요한 네트워크 인터페이스 비활성화, 실행코드 및 설정파일 무결성 검증, 장애 시 시스템 복원, 서비스 거부 공격 대응, 운영체제 기능 보호, 접근권한 최소화, 비인가 소프트웨어 설치·실행차단, 원격접속·네트워크 트래픽 통제
하드웨어 보안	안전한 부팅 및 자체시험, 자체시험 실패 시 대응, 하드웨어 장애 대응, 무단 훼손 방어, 부채널·메모리 공격 대응, 비휘발성 메모리 보호, 외·내부 인터페이스 보호

< IoT 보안인증 시험·인증 기준 >

IoT 보안 인증 제도를 취득하는 데 있어 이를 지원하는 컨설팅 서비스 보안 전문업체들이 있다. 보안 컨설팅 전문업체 컨설팅을 통해 발생 가능한 위협을 사전에 도출해 취약점 제거 및 대응 방안을 제시해 보다 안전하게 서비스 제공할 수 있도록 지원하고 있다.

마치며

업계에서는 5년 전부터 스마트 홈 기기와 관련하여 보안 위협을 경고해왔다. 그러나 보안 인식이 개선되지 않을 경우 결국 위와 같은 피해가 발생하며 이러한 보안 위협에 대응하기 위해 가장 중요한 것은 스마트 홈 기기의 보안 인식 개선이다.

국민 개개인과 제품 제조사, 건설업체, 정부 모두가 스마트 홈 기기에 대한 보안 인식 수준을 높여야 한다. 컨슈머 입장에서는 할 수 있는 보안 역할을 다하고, 건설 업체에서는 제품을 선정할 때 입주민들을 위한 보안 기준을 잘 정립하며, 제조사에서는 제품의 시스템에 대한 보안 인식을 강화하는 등 보안 인식을 개선하기 위한 노력이 필요하다.