OUCH! | 2018 년 8 월 호

OUCH!

SANS SECURITY AWARENESS

전 국민대상 월간 정보보호 인식제고 뉴스레터

스마트 홈 기기

스마트 홈 기기란?

과거에는 노트북, 스마트 폰 또는 게임 콘솔과 같이 집에 있는 일부 기기만 인터넷에 연결할 수 있었습니다. 그러나 오늘날에는 전구, 스피커, TV, 도어락, 심지어 자동차까지 점점 더 많은 기기가 인터넷에 연결됩니다. 곧 집안의 거의 모든 기기를 인터넷에 연결할 수 있게 됩니다. 이러한 연결된 기기는 종종 사물인터넷(IoT) 또는 스마트 홈 기기라는 이름으로 사용됩니다. 이러한 연결된 기기는 많은 편의를 제공하지만 고유한 위험도 존재합니다.

문제가 무엇인가?

가정의 네트워크에 연결된 기기가 많을수록, 위험도 커집니다. 해커는 기기를 조작하여 다른 사람을 공격하거나, 제조사가 광범위하게 우리의 활동 정보를 수집하거나, 기기가 감염되어 사용자가 접근할 수 없도록 잠글 수 있습니다. 이러한 기기를 제조하는 많은 회사는 사이버 보안에 대한 경험이 없으며 보안을 비용으로 간주합니다. 결과적으로 구입하는 기기 중 보안 기능이 거의 없거나 전혀 내장되어 있지 않습니다. 예를 들어, 일부 기기에는 잘 알려진 기본 패스워드가 설정되어 있거나, 새롭게 업데이트하거나 설정할 수 없습니다.

보호방법

그럼 어떻게 할 수 있을까요? 연결된 기기를 안전하게 사용해야 합니다. 이러한 기기는 인생을 더 단순하게 만들어 주는 멋진 기능을 제공할 수 있습니다. 또한 기술이 발전함에 따라 스마트 기기를 사용할 수밖에 없습니다. 다음은 자신을 보호하기 위해 취할 수 있는 주요 단계입니다.

필요한 것만 연결: 기기를 보호하는 가장 간단한 방법은 기기를 인터넷에 연결하지 않는 것입니다. 기기가 온라인 상태가 필요하지 않으면, 와이파이 네트워크에 연결하지 마십시오. 전화기에 알람을 보내는 토스터가 정말로 필요합니까?

연결된 기기 파악: 홈 네트워크에 어떤 기기가 연결되어 있습니까? 확실하지 않거나 기억할 수 없습니까? 무선 네트워크를 끄고, 어떤 것이 작동하지 않는 지 확인하십시오. 모든 것을 파악할 수는 없지만, 많은 기기가 우리가 모른 채 연결되어 있다는 것을 알게 되면 놀랄 것입니다.

업데이트 유지: 컴퓨터 및 모바일 기기와 마찬가지로 모든 기기를 최신 상태로 유지하는 것이 중요합니다. 기기에 자동 업데이트 할 수 있는 옵션이 있는 경우 사용하도록 설정하십시오.

패스워드: 기기의 패스워드는 사용자가 알고 있는 독특하고 강력한 패스워드로 변경하십시오. 이 때 한 번만 입력하면 됩니다. 모든 패스워드를 기억할 수 없다면, 패스워드 관리 프로그램을 사용하여 안전하게 저장하십시오.

개인 정보 옵션: 개인정보 옵션을 구성할 수 있는 기기가 있는 경우 수집하거나 공유하는 정보의 양을 제한하십시오. 하나의 옵션은 정보 공유 기능을 단순히 해제하는 것입니다.

제조사: 잘 알려져 있고 신뢰할 수 있는 회사로부터 기기를 구입하십시오. 보안을 지원하는 제품 (예: 자동 업데이트 기능, 기본 패스워드 변경 및 개인정보 설정 수정)을 구입하시기 바랍니다.

항상 청취: 기기가 음성 명령을 받을 수 있으면, 지속적으로 사람의 소리를 듣고 있습니다. 예를 들어, 알렉사 및 구글 홈 기기는 민감한 대화를 녹음할 수 있습니다. 가정에서 기기를 배치할 위치를 결정하고 개인정보 옵션을 검토할 때 이를 고려하십시오.

게스트 네트워크: 스마트 홈 기기를 컴퓨터 및 모바일 장치에 사용하는 기본 와이파이 네트워크가 아닌 별도의 "게스트" 와이파이 네트워크에 두는 것을 고려하십시오. 이렇게 하면 스마트 기기가 감염된 경우에도 주 네트워크의 컴퓨터나 모바일 기기는 안전합니다.

새로운 기술을 두려워할 필요는 없지만, 발생할 수 있는 위험을 이해해야 합니다. 위 몇 가지 간단한 단계를 수행하면 훨씬 더 안전하게 스마트 홈을 만들 수 있습니다.

한글판

본 문서는 한국의 ITL(http://www.itlkorea.kr)에서 번역하였습니다. ITL 은 미국 SANS 연구소의 한국 파트너로서 IT 거버넌스 및 IT 보안 분야의 최신의 지식과, 양질의 교육과 세미나를 진행하는 교육기관입니다. 추가적인 사항은 itl@itlkorea.kr 로 문의해주시기 바랍니다.

객원 편집자

로버트 리(@RobertMLee)는 SANS 공인 강사이며 FOR578 - 사이버 위협 인텔리전스 및 ICS515 - ICS 능동 방어 및 사고 대응 과정의 저자입니다. 로버트는 산업보안 회사인 '드래고스'의 CEO 겸 창립자이기도 하다.

참고자료

패스워드: https://www.sans.org/u/GEB

패스워드 관리프로그램: https://www.sans.org/u/GEG

홈 네트워크 보안: https://www.sans.org/u/GEL

 편집위원회: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | 번역: 진수희(ITL Inc.)