컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

OUCH!

이달 호 주제..

- 사물인터넷(IoT)란 무엇인가
- IoT 보안문제
- IoT 기기 보호방법

사물인터넷 (IoT)

사물인터넷(IoT)란 무엇인가?

과거에는 기술이 비교적 간단했습니다. 우리는 컴퓨터를 인터넷에 연결하고 일상 활동에서 사용하였습니다. 그리고 나서 기술이 스마트폰 및 태블릿과 같은 모바일 기기로 발전하면서 우리의 생활 속으로 들어왔습니다. 이러한 기기로 인해 일반 PC 컴퓨터가 주머니 속으로 들어왔습니다. 모바일 기기는 이동성이 훨씬 좋지만 자체 보안 문제가 있습니다. 다음 기술적인 큰 진보는 사물인터넷(IoT)입니다. 사물인터넷은 영문약어로IoT라고도 하며, 현관문 초인종, 전구에서부터 장난감, 온도계 등 모든 기기를 인터넷에 연결하는 것입니다. 이렇게 연결된 기기는 우리의 생활을 편리하게 만듭니다. 예를 들어 우리 스마트폰이 집으로 가까이 가면, 집의 전등이 자동으로 동작합니다. IoT 시장은 매주 새로운 기기가 나오면서 엄청난 속도로 움직이고 있습니다. 하지만 모바일 기기와 마찬가지로 IoT 기기도 자체 보안 문제를 가지고 있습니다. 이번 호에서는 IoT의 위험이 무엇인지, IoT 기기 및 가정 최종적으로 가족을 안전하게 지키는 방법에 대해서 다룹니다.

객원 편집자

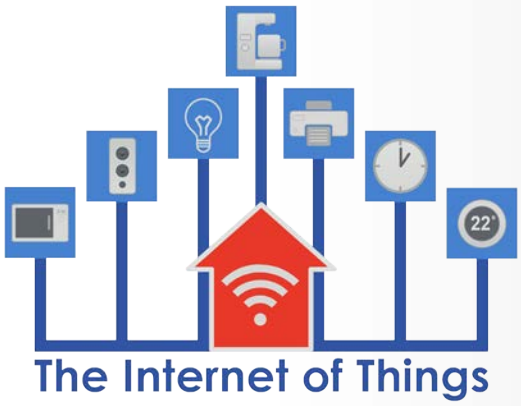
제임스 린(@jameslyne)은 보안연구소인 소포스(Sophos)의 글로벌 리더이다. 제임스의 기술적인 전문성은 다양한 보안분야로 확장하고 있다. 제임스는 SANS 연구소의 공인강사이며 산업계 컨퍼런스에서 주요 발표자로 활동하고 있다.

IoT 보안문제

IoT의 힘은 대부분의 기기들이 단순하다는 것입니다. 예를 들어, 커피 머신 코드를 연결하면, 커피머신이 가정 Wi-Fi 네트워크에 연결됩니다. 그러나 모든 단순함은 비용에서 옵니다. IoT 기기의 가장 큰 문제는 제조 기업들이 보안에 대해서 경험이 없으며, 회사의 전문성은 가정용 가전을 제조하는 것입니다. 또는 제조사들은 가장 효율적이고, 빠르게 제품을 개발하는 스타트업 기업입니다. 그 결과 많은 IoT 기기들이 제품에 보안기능이 거의 없습니다 예를 들어 일부 기기에는 잘 알려진 기본 패스워드가 설정되어 있으며, 패스워드 정보가 인터넷에 올라가 있으며, 변경도 할 수 없습니다. 추가로 이러한 많은 기기들은 재설정 기능도 없습니다. 더 나쁜 경우는 많은 기기들이 업데이트가 어려우며 업데이트 기능도

사물인터넷 (IoT)

없습니다. 그 결과 많은 IoT 기기들이 알려진 취약점이 존재하고 수정할 수도 없어 계속해서 취약한 상태로 존재합니다.



어떤 IoT 기기들이 홈 네트워크에 연결되었는지 확인하고, 가능하다면 분리를 해야합니다. IoT 기기를 업데이트하고, 강력한 패스워드로 보호해 주시기 바랍니다.

IoT 기기 보호방법

어떻게 해야 할까요? 우리는 IoT 기기의 힘을 안전하고 효과적으로 이용하기를 원합니다. 이러한 기기는 생활을 간편하게 만들고, 돈을 절약할 수 있고, 가정의 물리적 보안을 향상시킬 수 있는 기능을 제공합니다. 추가로 기술이 발전할수록 IoT기기를 어쩔 수 없이 선택하고 사용해야 합니다. 여기서는 IoT 기기와 우리를 보호할 수 있는 방법을 제시합니다.

- **필요한 것만 연결**: IoT 기기를 안전하게 하는 간단한 방법은 인터넷에 연결하지 않는 것입니다. 만약에 IoT 기기가 인터넷 연결이 필요 없다면, 와이파이에 연결하지 않는 것이 좋습니다.
- **별도의 와이파이 네트워크**: IoT 기기를 온라인 연결이 필요하다면, 별도의 와이파이 네트워크 사용을 고려하는 것이 좋습니다. 많은 와이파이 AP는 게스트 네트워크와 같은 추가적인 네트워크를 만드는 기능이 있습니다. 다른 방법은 IoT 기기만 접속할 수 있는 추가 와이파이 라우터를 구매하는 것도 좋습니다. 이렇게 하면 IoT 기기는 별도의 네트워크에 연결되어, 가정용 네트워크에 연결된 다른 컴퓨터나 기기는 공격 당할 위험이 줄어들게 됩니다.
- **가능하다면 업데이트 실시**: PC나 모바일 기기와 같이 IoT 기기도 업데이트가 필요합니다. 만약에 IoT기기가 자동 업데이트기능이 있으면 설정해 주시기 바랍니다.
- **강력한 패스워드**: IoT 기기에 유일하고, 강력한 패스워드로 변경해 주시기 바랍니다. 모든 패스워드를 기억하기 힘들다면, 패스워드 관리프로그램을 이용해서 패스워드를 안전하게 저장할 수 있습니다.
- **프라이버시 옵션**: IoT기기가 프라이버시 옵션을 설정할 수 있다면, 정보 공유를 제한해 두시기 바랍니다. 다른 방법은 정보 공유 기능을 모두 비활성화하는 것입니다.

사물인터넷 (IoT)

- **교체**: 사용하는 IoT 기기에 너무 많은 취약점이 있는데, 수정이 되지 않거나 좀 더 안전한 보안기능이 있는 신형 기기가 있다면, 새로운 것으로 교체하는 것도 좋습니다.

IoT 기기 보안방법에 대해서 모범 사례를 확인하고, 기사를 확인해 볼 필요가 있습니다. 하지만 대부분의 IoT 기기는 사이버보안을 고려하지 않고 만들어 졌습니다. 그래서 많은 제조사들이 충분한 보안 정보를 제공하지 않고 있습니다. 하지만 사이버보안에 대한 인식이 높아짐에 따라, 더 많은 IoT 제조사들이 자사 기기에 보안기술을 포함하고, 보호방법 및 업데이트 방법에 대한 정보를 제공해 줄 것을 기대합니다.

자세히 알아 보기

http://www.securingthehuman.org를 방문해서 OUCH! 뉴스레터를 읽어 보시고, 월간 OUCH! 정보보호지식 뉴스레터를 구독하십시오. 그리고 SANS 정보보호지식 솔루션에 대해서 좀 더 알아보시기 바랍니다.

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.

참고자료

패스워드:	https://securingthehuman.sans.org/ouch/2015#april2015
패스워드 관리프로그램:	https://securingthehuman.sans.org/ouch/2015#october2015
태블릿 컴퓨터 보안:	https://securingthehuman.sans.org/ouch/2016#january2016
홈 네트워크 보안:	https://securingthehuman.sans.org/ouch/2016#february2016

편집위원회 : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley, 번역: 진수희(ITL Inc.)