컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

OUCH!

이달 호 주제..

- 무선 네트워크
- 연결된 기기 보호

홈 네트워크 보안

개요

몇 년 전에홈 네트워크는 상대적으로 간단했습니다. 즉 인터넷 서핑, 온라인 쇼핑 및 게임 등을 위해 무선 AP와 컴퓨터 한 두 개가 전부였습니다. 하지만 홈네트워크는 굉장히 복잡해 졌습니다. 최근에는 네트워크에 훨씬 많은 기기들이 연결되어 있으며, 웹 브라우징 또는 미디어 시청 이상으로 사용하고 있습니다. 이번 호에서는 개인과 가족을 보호하기 위해 홈 네트워크를 안전하게 구축하는 방법을 다룰 예정입니다.

객원 편집자

체릴 콘리는 록히드 마틴에서 10만명의 직원을 대상으로 한 "I 캠페인"을 이용한 보안교육 및 인식제고를 담당하고 있다. 이 활동에는 글로벌 피싱 프로그램 뿐만 아니라 기업내 지원 그룹이 포함되어 있다. 트위터 @conleychera를 팔로우 하면 더 많은 정보를 얻을 수 있다.

무선 네트워크

거의 모든 홈 네트워크는 무선 네트워크(또는 와이파이 네트워크)를 가지고 있습니다. 이를 통해 노트북, 태블릿에서부터 게임 콘솔 및 TV 등 가정에 있는 기기를 인터넷에 연결시켜줍니다. 대부분의 가정용 무선 네트워크는 인터넷 라우터에서 의해서 통제됩니다. 이것은 인터넷에 연결하기 위해 가정에서 인터넷 서비스 회사들이 설치하는 기기입니다. 하지만, 일부 무선 네트워크 장비는 인터넷 라우터에 연결된 AP라고 불리는 별도의 시스템에 의해서 통제될 수 있습니다. 이 신호를 통해 가정에 있는 다른 기기들이 무선 네트워크에 연결합니다. 여기서 이러한 기기들은 인터넷에 연결할 수 있을 뿐만 아니라, 홈 네트워크에 있는 다른 기기에도 연결할 수 있습니다. 이 말은 무선 네트워크를 보호하는 것이 가정을 지키는 핵심부분입니다. 우리는 이를 보호하기 위해 아래의 단계를 권고합니다.

- 인터넷 라우터 또는 무선 AP의 기본 관리자 패스워드 변경. 이를 통해 무선 네트워크를 제어합니다. 관리자 계정을 통해 무선 네트워크를 설정할 수 있습니다. 문제는 많은 인터넷 라우터 또는 무선 AP는 기본 관리자 로그인 패스워드가 설정되어 있으며, 인터넷에 공개되어 있습니다. 즉 관리자 패스워드를 당신만 아는 강하고, 유일한 패스워드로 변경해야 합니다.
- 기본 무선 네트워크 이름(SSID) 변경. SSID는 연결하고 자 하는 기기들이 무선 네트워크를 검색하면 보게 되는 이름입니다. 쉽게 알아볼 수 있도록 홈 네트워크 이름을 유일한 이름으로 변경하는 것이 좋지만, 개인 정보가 포함된 것을 피하시기 바랍니다. 와이파이 네트워크 이름을 보이지 않도록(또는 브로드캐스트 하지 않도록)설정하는

홈 네트워크 보안

것은 거의 가치가 없는 일입니다. 최근에 와이파이 검색 도구를 이용하거나 실력 있는 공격자는 숨겨진 네트워크를 쉽게 찾을 수 있습니다.

- 믿을 수 있는 사람만 무선 네트워크에 연결하고, 사용하도록 해야 합니다. 그리고 보안을 강화해서 암호연결을 사용하도록 해야 합니다. 현재 가장 좋은 방법 중 하나가 WPA2 보안 메커니즘을 사용하는 것입니다. 이것을 적용시키면 와이파이 네트워크에 접속하는 사람들의 패스워드를 입력하도록 합니다. 일단 연결되면 온라인 활동은 암호화됩니다. 보안이 전혀 안되거나, 공개 네트워크인 WEP와 같은 구식 보안기술을 사용하지 말기바랍니다. 공개 네트워트는 인증없이 누구나 와이파이 네트워크에 접근할 수 있습니다.
- 와이파이 네트워크에 접속하기 위해 사용하는 패스워드를 설정할 때는 관리자 패스워드와 다른 것을 사용하고, 강력한 것을 선택하기 바랍니다. 장비를 통해 와이파이 접근할 때 한번만 입력하면 되고, 다음에 접속할 때는 패스워드를 기억하고 있습니다.

홈 네트워크를 보호하기 위해서는 무선 네트워크를 보호하고, 업데이트하고, 모든 기기에 패스워드를 설정하시기 바랍니다.

- 많은 무선 네트워크는 게스트 네트워크를 지원합니다. 이것은 방문자들이 인터넷에 연결할 수 있도록 하지만, 홈 네트워크의 다른 기기에는 접속할 수 없어 보호기능이 있습니다. 만약에 게스트 네트워크를 추가하면, WPA2 암호를 설정하고 유일한 패스워드를 설정하시기 바랍니다.
- 패스워드 및 설정 옵션을 알지 못한 채 새로운 기기들이 네트워크에 연결을 허용할 수 있는 기능을 설정하지 마시기 바랍니다.
- 너무 많은 패스워드를 기억하기 힘들다면, 패스워드를 저장 및 관리하는 패스워드 관리프로그램을 이용하기를 권고합니다.

위 단계가 어렵다면, 인터넷 서비스 회사에 문의하거나, 인터넷 라우터 또는 무선 AP에 따라오는 설명서나 제조사 웹사이트를 참조 바랍니다.

연결된 기기 보호

다음 단계는 누가 홈네트워크에 연결되어 있는 지, 연결된 기기가 안전한지를 확인하는 것입니다. 기기가 몇대 연결되어 있지 않았을 때는 이 단계는 간단했습니다. 요즘은 “항상 연결”된 세상이고, TV, 게임 콘솔, 베이비 모니터, 스피커,

홈 네트워크 보안

온도계 심지어 자동차까지 대부분의 기기들이 홈 네트워크에 연결할 수 있습니다. 홈 네트워크에 연결되어 있는 것을 찾는 쉬운 방법은 Fing과 같은 것으로 스캐닝하는 것입니다. 이 앱을 컴퓨터나 모바일 기기에 설치해서 무선 네트워크를 스캔하면 연결되어 있는 모든 기기를 보여줍니다. 일단 홈 네트워크에 연결된 모든 기기를 식별했다면, 이 기기들이 안전한 것을 확인해야 합니다. 가장 좋은 방법은 운영체제/펌웨어 버전을 최신으로 유지하는 것입니다. 가능하다면, 자동 업데이트 기능을 사용바랍니다. 만약에 어떤 기기가 패스워드 입력을 요구하면, 유일하고 강한 패스워드를 사용 바랍니다. 마지막으로 홈 네트워크를 안전하게 구성할 수 있는 도구를 제공할 수 있으니 인터넷 서비스 회사 웹 사이트를 방문해 보시기 바랍니다.

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 매핑:	http://l.rud.is/home-network-mapping

편집위원회 : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner, 번역: 진수희(ITL Inc.)