OUCH! | 2014 년 1월호

컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

OUCH!

이달 호 주제..

- 무선 네트워크 보안
- OpenDNS
- 단말기 보안

홈 네트워크 보안

개요

몇 년 전만해도 홈 네트워크는 비교적 간단했다. 즉 인터넷 서핑, 온라인 게임을 위한 단순히 무선 라우터 한대와 컴퓨터 1, 2대를 같이 사용했다. 하지만 지금은 홈 네트워크가 계속 복잡해 지고 있다. 홈 네트워크에 점점 더 많은 기기들이 연결되고 더 많은 것을 하고 있다. 이번 호에서는 홈 네트워크를 좀 더 안전하게 만드는 기본적인 단계를 다룬다.

객원 편집자

케빈 존슨은 시큐어 아이디어社 CEO이며 MySecurityScanner.com을 운영하고 있으며, SANS 연구소 선임강사이다. www.secureideas.com을 방문하면 더 많은 정보를 알 수 있다.

무선 네트워크 보안

거의 모든 홈 네트워크가 무선 네트워크(와이 파이 네트워크)에서 시작한다. 무선 네트워크를 이용하면 무선으로 노트북, 태블릿뿐만 아니라 게임기, TV 등 다양한 기기를 등 인터넷에 연결할 수 있다. 이를 위해 무선 네트워크는 무선 AP가 필요하다. 무선 AP는 물리적인 기기로 인터넷 라우터로 연결해주는 것이다. 그리고 기기가 연결하고자 하는 무선 신호를 보낸다. 기기들이 AP에 접속하면, 인터넷뿐만 아니라 홈 네트워크에 다른 기기로 연결할 수 있다. 그 결과 무선 AP는 홈 네트워크의 중요 부분 중 하나이기 때문에 이를 보호하기 위해 다음 단계를 추천한다.

- 대부분의 무선 AP의 기본 관리자 로그인 및 패스워드는 잘 알려져 있는 것이고, 인터넷에 공개되어 있기도 하다. 그래서 반드시 기본 관리자 패스워드는 변경을 해야 한다. 패스워드를 만들 때는 다른 계정에서 사용되고 있는 것 외에 새로운 것으로 만들어야 한다.
- 또 다른 문제는 무선 AP 이름(SSID)을 정하는 것이다. SSID는 기기들이 무선 네트워크를 찾을 때 사용되는 이름이다. 이름을 정할 때 다른 것과 중복되지 않게 하여 쉽게 찾을 수 있는 것으로 해야 한다. 하지만 개인 정보가 포함되어서는 안 된다. 또한 대부분의 무선 스캔 도구 또는 공격자는 쉽게 숨겨진 네트워크를 찾아낼 수 있기 때문에 SSID를 숨기는 것은 큰 효과가 없다.

홈 네트워크 보안

- 다음 단계는 아는 사람 및 신뢰할 수 있는 사람만 무선 네트워크에 접속할 수 있도록 해야 한다. 그리고 네트워크 통신은 암호화해야 한다. 이웃 주민 또는 모르는 사람들이 네트워크에 연결하지 못하게 해야 한다. 이를 위해 무선 AP 설정 시 강력한 보안을 설정하면 이러한 위험을 예방할 수 있다. 현재 가장 좋은 방법은 WAP2 암호 메커니즘을 사용하는 것이다. 접속 시 암호를 입력하게 해 놓으면, 인증이 되면 통신이 암호화된다. 그리고 WEP와 같은 오래된 암호 메커니즘을 사용하거나, 암호를 사용하지 않는 것은 위험하다. 네트워크를 공개하면 인증 없이 모든 사람들이 무선 네트워크에 접속할 수 있다.
- 무선 네트워크 접속을 위해 설정하는 패스워드는 다른 관리자 패스워드와는 다른 추측하기 힘들고, 강도가 높은 것을 설정해야 한다. 또한 패스워드는 기기마다 다른 것을 사용해야 한다는 점을 명심해야 한다.
- 많은 무선 AP는 게스트 네트워크를 지원한다. 게스트 네트워크는 방문자들이 무선 네트워크에 접속하여 인터넷에 접근할 수 있지만 홈 네트워크에 있는 내부 기기에는 접속할 수 없다. 만약에 게스트 네트워크를 추가하려면 WPA2를 사용하고 패스워드도 다른 것을 설정해야 한다.
- 다양한 패스워드를 기억하지 못한다면, 패스워드 관리 프로그램을 이용해서 안전하게 저장하는 것이 좋다.

가정용 네트워크를 보호하기 위해서 무선 네트워크를 안전하게 구성하고, OpenDNS를 사용하고, 연결된 모든 기기 운영체제가 최신의 버전으로 업데이트되도록 해야 한다.

OpenDNS

일단 무선 네트워크를 설정하면, DNS서버로 OpenDNS를 사용할 것을 권고한다. DNS는 브라우저에서 이름을 입력하면 브라우저가 인터넷에 연결해야할 서버를 알려주는것이다. OpenDNS 서비스는 감염된 웹 사이트를 알려주고, 모르고 감염된 웹사이트를 방문시 가정용 무선 네트워크에서 접속을 차단하는 역할을 한다. 추가로 이러한 서비스는 이상한 웹 사이트를 필터링하고 차단하는 기능도 제공한다. 이 기능이 좋은 점은 기기에 아무것도 설치하지 않아도 되며, 무선 AP에 설정만 하면 된다.

홈 네트워크 보안

단말기 보안

다음단계는 어떤 단말기들이 홈 네트워크에 접속되어 있는 지, 이러한 기기들이 안전한 지를 확인해야 한다. 일반적으로 몇 개 안 되는 기기들이 연결되어 있다면 이것은 큰 문제가 없다. 하지만 매일 매일 TV, 게임 콘솔, 유아 모니터기, 스피커 및 가정용 온도계 또는 자동차 등 모든 것이 연결될 수 있다. 가정용 네트워크에 연결된 모든 기기를 확인해보면 굉장히 놀랄 수 도 있다. 이러한 기기들을 안전하게 유지하기 위해서는 기기들의 운영체제가 최신 버전으로 사용되고 있어야 한다. 이를 위해서는 자동 업데이트 기능을 설정할 수 있다. 자동 업데이트 기능이 없다면, 월 1회 업데이트해야 한다. 추가로 인터넷 서비스 회사 웹사이트를 방문해서 가정용 네트워크를 안전하게 구성할 수 있는 도구나 서비스가 있으면 사용할 수 있다.

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

OpenDNS:
http://www.opendns.org
Norton ConnectSafe:
http://dns.norton.com/dnsweb/dnsForHome.do
네트워크 보안 스캐너:
http://www.sophos.com/en-us/products/free-tools/network-security-scan.aspx
패스워드 관리프로그램:
http://www.securingthehuman.org/resources/newsletters/ouch/2013#october2013

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