SANS SECURITY AWARENESS
ITL TRAINING LEADERS
OUCH! | 2018 년 01월 호
전 국민대상 월간 정보보호 인식제고 뉴스레터

OUCH!

이달 호 주제..

- 무선네트워크
- 단말기 연결
- 패스워드
- 백업

홈 사이버보안 구축

개요

몇 년 전에는 가정의 보안은 간단했습니다. 즉 대부분의 가정은 하나의 무선 네트워크와 여러 대의 컴퓨터로 구성되어 있었습니다. 하지만 기술이 훨씬 더 복잡해졌으며, 많은 일상생활이 모바일 기기, 게임 콘솔 뿐만 아니라 온도계 심지어 냉장고까지 기술과 통합되고 있습니다. 이번 호에서는 가정의 사이버보안을 지키기 위한 4단계를 설명합니다.

객원 편집자

맷 브로밀리는 다양한 규모의 고객에 대해서 데이터 침해사고를 해결하는 사고대응전문가입니다. 맷은 또한 SANS 강사이며, FOR508 고급 디지털 포렌식 및 사고대응 과정을 가르칩니다. Matt @mbromileyDFIR 를 팔로우하십시오.

무선 네트워크

거의 모든 홈 네트워크는 무선 네트워크(또는 와이파이 네트워크)를 가지고 있습니다. 이를 통해 가정에 있는 모든 기기를 인터넷에 연결시켜줍니다. 대부분의 가정용 무선 네트워크는 인터넷 라우터 또는 독립적인 무선 AP에 의에서 통제됩니다. 둘 다 무선 신호를 브로드캐스팅하여 집에 있는 기기는 이러한 신호를 통해 연결됩니다. 이 말은 무선 네트워크를 보호하는 것이 가정의 보안을 지키는 핵심입니다. 우리는 이를 보호하기 위해 아래의 단계를 권고합니다.

- 가정의 무선 네트워크를 제어하는 인터넷 라우터 또는 무선 AP의 기본 관리자 패스워드 변경. 관리자 계정을 통해 무선 네트워크를 설정할 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 사람들은 패스워드를 입력해야 합니다. 일단 연결되면 온라인 활동은 암호화됩니다.
- 와이파이 네트워크에 접속하기 위해 사용하는 패스워드를 설정할 때는 관리자 패스워드와 다른 것을 사용하고, 강력한 것을 선택하기 바랍니다. 각각의 기기를 통해 와이파이 접근할 때 한번만 입력하면 되고, 다음에 접속할 때는 패스워드를 기억하고 있습니다.
- 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.

홈 사이버보안 구축

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

다음 4 가지 간단한 단계에 따라 사이버 보안 가정을 만듭니다. Wi-Fi 네트워크 보안, 자동 업데이트 활성화, 고유 한 암호문 사용 및 백업 활성화 등이 있습니다.

단말기 연결

다음 단계는 누가 홈네트워크에 연결되어 있는 지, 연결된 기기가 안전한지를 확인하는 것입니다. 기기가 몇 대 연결되어 있지 않았을 때는 이 단계는 간단했습니다. 요즘은 “항상 연결”된 세상이고, TV, 게임 콘솔, 베이비 모니터, 스피커, 온도계 심지어 자동차까지 대부분의 기기들이 홈 네트워크에 연결할 수 있습니다. 일단 홈 네트워크에 연결된 모든 기기를 식별했다면, 이 기기들이 안전한 것을 확인해야 합니다. 가장 좋은 방법은 가능하다면, 자동 업데이트 기능을 사용하시기 바랍니다. 사이버 공격자는 서로 다른 장치와 운영 체제에서 끊임없이 새로운 약점을 찾고 있습니다. 자동 업데이트를 사용하면 컴퓨터와 장치가 항상 최신 소프트웨어를 실행하므로 다른 사람이 해킹하기가 더 어려워집니다.

패스워드

다음 단계는 기기별, 온라인 계정별 강력하고 고유한 패스워드를 사용하는 것입니다. 여기서 중요한 것은 패스워드는 강력하고, 독특해야 합니다. 강력한 패스워드를 만들고자 기억하기 어렵고 입력하기 어려운 복잡한 패스워드를 가지고 있다면, 대신 패스워드 문구를 사용하십시오. 이것은 “내 커피는 어디 있습니까?”또는 “햇빛-도넛 - 행복 - 분실”과 같이 쉽게 기억할 수 있는 일련의 단어를 사용하는 패스워드 유형입니다. 패스워드 문구는 길수록 강해집니다. 고유한 패스워드는 각각의 기기 및 온라인 계정에 다른 패스워드를 사용한다는 것을 의미합니다. 이렇게 하면 하나의 패스워드가 유출되더라도 다른 계정과 기기가 여전히 안전합니다. 강력하고 고유한 패스워드를 모두 기억할 수 없다면, 암호화된 가상 금고에 모든 패스워드를 안전하게 저장하는 특별한 보안 프로그램인 패스워드 관리프로그램을 사용하는 것이 좋습니다.

마지막으로, 특히 온라인 계정에 사용할 수 있을 때마다 2 단계 인증을 사용하십시오. 2 단계 인증이 훨씬 강력합니다. 패스워드를 사용하지만 스마트 폰으로 전송된 코드나 코드를 생성하는 스마트 폰의 앱과 같은 두 번째 단계를 추가합니다. 2 단계 인증은 온라인에서 자신을 보호하기 위해 취할 수 있는 가장 중요한 유일한 단계 일 것입니다. 생각보다 훨씬 쉽습니다.

홈 사이버보안 구축

백업

아무리 조심스럽게도 해킹 당할 수 있습니다. 이 경우 개인 정보를 복구 할 수 있는 유일한 방법은 백업에서 복구하는 것입니다. 중요한 정보를 정기적으로 백업하고 복원할 수 있는지 확인하십시오. 대부분의 모바일 기기는 클라우드에 자동 백업을 지원합니다. 대부분의 컴퓨터에서는 비교적 저렴한 가격에 사용하기 쉬운 백업 소프트웨어 또는 서비스를 구입해야 할 수 있습니다.

자세히 알아 보기

securingthehuman.sans.org/ouch/archives를 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/2017#april2017
패스워드 관리프로그램: https://securingthehuman.sans.org/ouch/2017#september2017
Stop|Think|Connect: https://securingthehuman.sans.org/ouch/2017#december2017
구글 2단계 인증: https://securingthehuman.sans.org/ouch/2017#august2017

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