OUCH! | 2016 년 10 월호

전 국민대상 월간 정보보호 인식제고 뉴스레터

OUCH!

이달 호 주제..

- 우리자신
- 패스워드
- 보안 업데이트
- 백업

핵심 보안 4단계

개요

기술이 우리 생활에 중요한 역할을 하고 있으며, 또한 복잡도 증가하고 있습니다. 기술이 급격히 변하는 상황에서 보안 권고사항을 지키는 것이 혼란스럽습니다. 무엇을 해야 할지, 무엇을 하지 말아야 할 지에 대해서 항상 새로운 가이드가 나옵니다. 하지만 보안을 지키는 상세 방법을 매번 변하지만 우리를 지키기 위한 기본적인 사항은 존재합니다. 어떤 기술을 사용하던지, 어디에 있던지 상관없이, 다음의 보안 4단계를 권고합니다. 아래 단계에 추가적인 사항을 알고 싶다면, 이 뉴스레터의 끝에 있는 참고자료를 읽어보시기 바랍니다.

객원 편집자

라이언 존슨은 조직이 방어할 수 없는 침해사고를 준비할 수 있도록 하는 일을 하고 있으며, SANS 연구소에서 고급 네트워크 포렌식을 강의한다. 라이언은 트위터 @ForensicRJ을 사용하면서 활동한다.

1. **우리자신**: 가장 먼저 기술로만 우리 자신을 완전히 보호할 수 없다는 점을 명심하시기 바랍니다. 공격자들은 최신의 보안기술을 우회할 수 있는 가장 쉬운 방법은 우리를 통해서 공격하는 것입니다. 공격자들이 패스워드, 신용카드 정보 및 개인정보를 원한다면, 이를 획득할 수 있는 가장 쉬운 방법은 우리를 속여서 이러한 정보를 공격자에게 주는 것입니다. 예를 들어 공격자들이 전화해서 삼성전자 기술 지원팀이라고 해서, 컴퓨터/스마트폰이 감염되었다고 주장합니다. 실제 이것은 우리 컴퓨터나 스마트폰에 접근하려고 하는 범죄자입니다. 또는 쇼핑몰에서 구매한 물건이 배달이 되지 않다고 하면 이메일 보내서, 이메일 주소를 확인하라며 링크를 클릭하도록 요구할 수 있습니다. 하지만 실제로는 우리를 속여서 악성 웹사이트를 방문하도록 하여 컴퓨터를 해킹하는 것입니다. 이것은 랜섬웨어 또는 CEO 사기를 위한 공격방법입니다. 극단적으로 공격자에 대한 최고의 방어는 우리자신입니다. 의심을 해 보시기 바랍니다. 상식에 따라 판단하면 대부분의 공격을 발견하고 저지할 수 있습니다.

2. **패스워**드: 우리를 보호할 수 있는 다음 단계는 컴퓨터/온라인 서비스별로 강력하고 유일한 패스워드를 사용하는 것입니다. 여기서 키워드는 “강력”하고 “유일”한 것입니다. 강력한 패스워드는 자동화 프로그램을 통해 해커들이 쉽게 추측할 수 없는 것입니다. 기억하기 어려운 복잡한 패스워드 설정이 힘드십니까? 그렇다면 패스워드 문구를 이용해서

핵심 보안 4단계

보십시요. 간단한 단어 대신에 “내 커피가 어디있지?” 와 같이 기억하기 쉬운 문장을 사용하는 것입니다. 패스워드 문구를 길게 만들수록 더 강력해집니다. 유일한 패스워드란 컴퓨터 및 온라인 서비스별로 다른 패스워드를 사용하는 것을 의미합니다. 이 방법을 사용하면 하나가 해킹되어도 다른 계정은 안전하게 됩니다. 강력하고, 유일한 패스워드를 기억하기 어렵다구요? 하지만 걱정마십시요. 대부분의 사람들이 그렇습니다. 그렇다면 패스워드 관리프로그램을 이용해 보십시요. 이것은 스마트폰 또는 컴퓨터의 특별한 프로그램으로 모든 패스워드를 암호화여 저장하여 사용할 수 있습니다.

보안 4단계를 따르면, 최신의 기술을 이용하면 우리를 확실히 보호할 수 있습니다.

마지막으로 패스워드 보안을 위해 가장 중요한 단계 중 하나는 2단계 인증을 사용하는 것입니다. 패스워드만으로 더 이상 계정을 보호하기 위해 충분하지 않습니다. 좀 더 강력한 것이 필요합니다. 2단계 인증은 훨씬 강합니다. 이것은 패스워드를 사용하지만, 두 번째 단계가 추가됩니다. 즉 생체인식 또는 스마트폰으로 보내거나, 스마트폰 앱에서 생성하는 코드를 추가적으로 이용합니다. 우리가 사용하는 계정에서 패스워드 관리프로그램 등 이러한 기능을 활성화해서 사용해 보십시요. 2단계 인증은 우리를 보호할 수 있는 유일한 또는 가장 중요한 단계이며, 사용하기에도 편리합니다.

3. **업데이트**: 컴퓨터, 모바일 기기 앱 등 인터넷에 연결되어 사용되고 있다면 최신의 소프트웨어를 사용하도록 해야 합니다. 사이버범죄자들은 지속적으로 우리가 사용하는 소프트웨어의 새로운 취약점을 찾고 있습니다. 이러한 취약점을 찾으면, 이를 공격하기 위해 특별한 프로그램을 이용해서 우리가 사용하고 있는 컴퓨터/스마트폰을 해킹합니다. 그러는 동안 이러한 기기의 소프트웨어를 만든 회사들은 취약점을 수정하는 업데이트를 배포하기 위해서 일합니다. 최신의 소프트웨어를 이용하기 위해서는 자동 업데이트 기능을 설정해 주시기 바랍니다. 이 규칙은 인터넷 연결된 TV, 베이비 모니터, 가정용 라우터, 게임 콘솔 또는 향후 자동차 등 네트워크에 연결되는 모든 기술에 적용됩니다. 만약에 운영체제 또는 기기들이 너무 오래되어서 보안 업데이트를 지원하지 않는다면, 업데이트를 지원하는 새로운 것을 교체할 것을 권고합니다.

핵심 보안 4단계

4. **백업**: 하지만, 아무리 조심하더라도 해킹 당할 수 있습니다. 해킹 당한다면, 컴퓨터/스마트폰이 악성코드가 없다고 확신할 수 있는 유일한 방법은 완전히 삭제하고 새로 설치하는 것입니다. 공격자들은 해킹한 시스템에 저장되어 있는 개인적인 파일, 사진에 우리가 접근하는 것을 막을 수 있습니다. 그렇다면 개인적인 정보를 복구할 수 있는 유일한 방법으로 백업한 파일에서 복구하는 것입니다. 그래서 중요한 정보는 정기적인 백업을 해야 하며, 복구가 되는 지 확인해야 합니다. 대부분의 운영체제 및 스마트폰은 자동 백업을 지원합니다. 추가로 사이버 공격자로부터 자료를 보호하기 위해 클라우드 또는 오프라인에 백업자료를 저장할 것을 권고합니다.

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

피싱:	https://securingthehuman.sans.org/ouch/2015#december2015
패스워드 관리프로그램:	https://securingthehuman.sans.org/ouch/2015#october2015
2단계 인증:	https://securingthehuman.sans.org/ouch/2015#september2015
패스워드:	https://securingthehuman.sans.org/ouch/2015#april2015
백업:	https://securingthehuman.sans.org/ouch/2015#august2015

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