컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

OUCH!

이달 호 주제..

- 개요
- 핵심 보안 5단계

핵심 보안 5단계

개요

기술이 우리 생활에 점점 더 중요한 역할을 하게 되면서, 기술의 복잡도도 증가하고 있다. 기술이 너무 빨리 변함에 따라 보안을 유지하는 것이 어려운 일이 되고 있다. 해야할 것과 하지 말아야 할 것에 대해서 새로운 가이드가 계속 나오고 있다. 하지만 보안을 지키는 상세 방법이 항상 변하지만, 우리를 보호하기 위한 근본적인 방법은 변하지 않는다. 우리 어떤 기술을 이용하던지, 어디서 이용하던지, 여기서는 다음과 같은 5단계 핵심 단계를 권고한다.

객원 편집자

레니 젤트서는 NCR사의 IT 운영 보안을 하고 있으며, SANS 연구소에서 악성코드 과정을 강의하고 있다. 레니는 트위터 @lennyzeltser에서 활동하고 있으며, blog.zeltser.com에서 보안 블로그를 운영하고 있다.

핵심 5단계

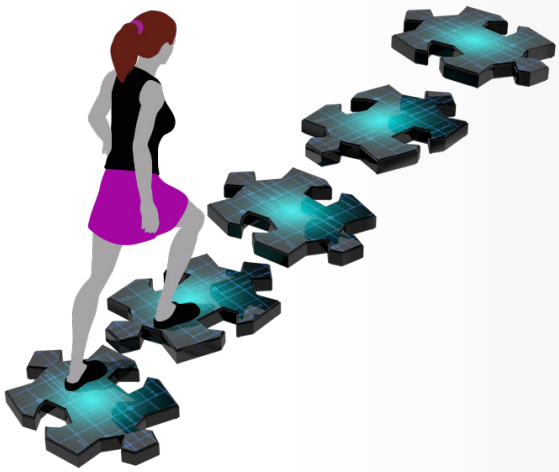
아래 설명하는 각각의 단계는 간단한 개요이다. 각 단계에 대해서 좀더 알고 싶다면, 본 뉴스레터 끝에 있는 참고자료를 참고하기 바란다.

1. **우리**: 가장 먼저, 기술자체로는 우리를 보호할 수 없다. 공격자는 뛰어난 보안 기술을 우회할 수 있는 가장 쉬운 방법은 바로 사람을 공격하는 것이라는 것을 알게 되었다. 만약에 공격자들이 패스워드 또는 신용카드 정보를 원한다면, 사람을 속여서 정보를 주도록 만드는 것이다. 예를 들어 “KT 기술지원팀”이라고 전화해서 컴퓨터가 감염되었다고 한다. 하지만 실제로는 컴퓨터에 접근하기 위해 속이는 사이버 범죄자이다. 또는 만약에 공격자들이 이메일을 발송한 후 주문한 물건이 배송되지 않는다고 하며, 주소를 확인하기 위해 링크를 클릭하도록 요청한다. 이것도 실제로는 악성 웹 사이트를 방문하도록 만들어 컴퓨터를 해킹하고자 하는 것이다. 극단적으로 공격자에 대한 최고의 방어는 바로 우리이다. 일반적인 공격을 찾고 방어하기 위해서는 상식에 맞게 판단해야 한다.

2. **업데이트**: 인터넷에 연결되는 컴퓨터, 모바일 기기, 앱 등은 최신의 소프트웨어로 운영되도록 해야한다. 사이버 범죄자들은 사람들이 사용하는 기술에 대한 지속적으로 취약점을 찾고 있다. 사이버 범죄자들이 이러한 취약점을 찾게 되면, 특수 제작한 프로그램을 이용해서 취약점을 공격한 후 네트워크, 컴퓨터 및 모바일 기기 등 우리가 사용하고

핵심 보안 5단계

있는 모든 기술을 해킹할 수 있다. 우리가 사용하고 있는 기술을 개발한 회사들은 항상 업데이트를 유지하고자 한다. 일단 취약점이 알려지면, 회사에서는 이를 고치기 위해 패치를 개발하여 공개한다. 컴퓨터 및 모바일 기기들이 이러한 업데이트를 설치하였는지 확인하여 알려진 취약점 수를 줄여 공격할 수 있는 가능성을 낮춰야 한다. 최신의 소프트웨어로 유지하기 위해서는, 가능하다면 자동 업데이트로 설정하는 것이 좋다. 이 규칙은 인터넷 TV, 어린이 모니터, 가정용 무선 라우터, 게임 콘솔뿐만 아니라 자동차 등 인터넷에 연결되는 거의 모든 기술에 적용된다. 만약에 우리가 사용하고 있는 컴퓨터의 운영체제, 모바일 기기 또는 다른 기술이 더 이상 업데이트를 지원하지 않는다면, 업데이트를 지원하는 신규 제품을 사용할 것을 권고한다.



5단계 보안을 지키면, 최신의 기술을 이용하는 동안 우리자신을 보호할 수 있습니다.

3. **패스워드**: 우리를 보호할 수 있는 세 번째 단계는 IT 기기, 온라인 계정 및 애플리케이션별로 서로 다른 "강력하고, 유일한" 패스워드를 사용하는 것이다. 여기서 핵심단어는 "강력하고 유일한" 것이다. 강력한 패스워드는 해커 또는 자동 프로그램에 의해서 쉽게 추측되지 않는 것이다. 하나의 단어를 이용하는 것 보다, 기호 및 특수 문자를 포함하여 복수의 단어를 사용하는 것이 좋다. "유일한"의 의미는 기기 및 온라인 계정마다 서로 다른 패스워드를 사용하는 것이다. 이렇게 하면 패스워드 하나가 해킹되어도, 다른 계정의 패스워드 및 기기는 안전하게 된다. 강하고, 유일한 패스워드가 너무 많아서 기억하기 어렵다면, 걱정할 필요가 없다. 대부분 사람들은 기억하기 어렵다. 그래서 여기서는 패스워드 관리 프로그램을 이용할 것을 권고한다. 이것은 스마트폰 또는 컴퓨터의 패스워드를 암호화하여 안전하게 저장하는 특별한 프로그램이다. 마지막으로 만약에 어떤 계정에서는 2단계 인증을 지원한다면, 항상 이것을 사용할 것을 권고한다. 왜냐하면 이 방법이 계정을 보호할 수 있는 가장 강력한 방법 중 하나이다.

4. **암호**: 네 번 째 단계는 암호를 사용하는 것이다. 암호는 우리 또는 우리가 신뢰하는 사람만이 우리의 정보에 접근할 수 있도록 한다. 데이터 암호화는 전송 및 저장 시 두 가지 방법으로 암호화가 가능하다. 저장 데이터를 암호화하는 것은 하드 디스크 또는 USB 스틱과 같이 파일로 저장되어 있는 것을 보호하는 것이다. 대부분의 운영체제는 전체디스크 암호화(FDE)와 같은 기능을 이용해서 모든 데이터를 자동적으로 암호화하는 기능이 있다. 전송 데이터 암호화는 온라인 뱅킹할 때와 같이 컴퓨터에서 다른 기기로 전송될 때 데이터를 암호화하는 것이다. 웹 브라우저를 사용하면서

핵심 보안 5단계

암호화가 적용되는 지 확인할 수 있는 방법은 방문하는 웹 사이트의 주소가 “https:”로 시작하며, 그 옆에 잠금된 자물쇠 이미지가 나타난다.

5. **백업**: 마지막으로 아무리 조심한다고 하더라도, 가끔 IT 기기 또는 계정 중 하나가 해킹될 수 있다. 이런 경우 컴퓨터나 모바일 기기에 악성코드가 없다는 것을 확인할 수 있는 가장 확실한 방법은 완전히 지우고, 다시 설치하는 것이다. 공격자들이 종종 해킹된 시스템에 있는 개인적인 파일, 사진 등의 정보에 접근할 수 없도록 설정하기도 한다. 이런 경우 백업된 데이터를 이용해야만 컴퓨터나 모바일 기기에 저장된 정보를 복구할 수 있다. 그래서 모든 중요한 데이터는 복구할 수 있도록 정기적으로 백업을 해야 한다. 대부분의 운영체제 및 모바일 기기는 자동 백업을 지원한다.

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

이메일 피싱 공격:	http://www.securingthehuman.org/ouch/2013#february2013
태블릿 안전하게 유지하기:	http://www.securingthehuman.org/ouch/2013#december2013
강한 패스워드:	http://www.securingthehuman.org/ouch/2013#may2013
패스워드 관리프로그램:	http://www.securingthehuman.org/ouch/2013#october2013
2단계 인증:	http://www.securingthehuman.org/ouch/2013#august2013
암호:	http://www.securingthehuman.org/ouch/2014#august2014
백업:	http://www.securingthehuman.org/ouch/2013#september2013

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