OUCH! | 2015 년 9 월호

컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

OUCH!

이달 호 주제..

- 개요
- 패스워드
- 2단계 인증

2단계 인증

개요

우리가 누구인지(인증)를 검증하는 프로세스는 개인의 정보를 보호하기 위한 중요한 방법이다. 이메일, 사진, 은행 계좌와 같이 우리들만의 개인 정보를 접근하기 위해서는, 우리가 누구인지를 증명하기 위해 강력한 인증을 사용해야 한다. 자신을 증명하기 위해서는 3가지 방법이 있다. 즉 패스워드와 같이 우리가 알고 있는 것, 운전면허증과 같이 우리가 가지고 있는 것, 지문과 같이 우리가 가지고 있는 유일한 것이 있다. 이러한 방법은 각각 장점과 단점이 있다. 가장 일반적인 인증 방법은 패스워드와 같이 우리가 알고 있는 것을 이용하는 것이다. 이번 뉴스레터에서는 여전히 많이 사용되고 있는 단순 패스워드보다 훨씬 안전한 2단계 인증을 이용해서 우리를 보호하는 방법을 설명한다.

객원 편집자

케이스 팜그렌은 정보보호분야에 30년의 경력을 가지고 있다. 케이스는 SANS 공인강사이며, SEC301 과정 저자이다. 강의를 하지 않을 때는 케이스는 컨설팅 및 프로젝트를 진행하고 있다. 트위터 계정은 @kpalmgren이다.

패스워드

패스워드는 우리가 알고 있는 것을 기반으로 우리가 누구인 지를 증명하는 것이다. 패스워드가 가지고 있는 위험은 패스워드는 단일장애점(SPOF)이라는 것이다. 누군가 우리의 패스워드에 접근하거나 추측할 수 있다면, 신분을 위장하고 패스워드로 보호된 모든 정보에 접근이 가능하다. 그래서 공격자들이 추측하기 어렵게 하고, 계정마다 다른 패스워드를 사용하고, 다른 사람과 공유하지 않는 등의 패스워드를 보호하는 방법을 배워야 한다. 이러한 권고가 유효하지만, 패스워드는 유용성보다 더 오랫동안 존재하며, 최근 시대에는 더 이상 효과적이지 않다. 새로운 기술이 발달함에 따라 사이버 공격자들은 더 쉽게 패스워드를 해킹할 수 있다. 우리가 필요한 것은 쉽게 사용할 수 있기도 하며, 강력한 인증을 위해 간단하지만 좀 더 안전한 방법이 필요하다. 다행히도 최근에 2 단계 인증이라는 방법이 많이 사용되고 있다.

2단계 인증

2단계 인증(2중 인증)은 단순한 패스워드 보안 더 안전한 방법이다. 인증하기 위해 단 한 번만 인증을 요구하지 않고, 서로 다른 2가지 방법을 요구한다. ATM 카드가 그 예이다. 우리가 ATM 기기에서 돈을 인출할 때, 실제로

2단계 인증

2단계 인증을 사용하고 있다. 돈에 접근할 때 2가지를 해야 한다. ATM 카드(우리가 가지고 있는 것)과 PIN 번호(우리가 알고 있는 것)이다. ATM 카드를 분실해도 돈은 안전하다. 카드를 주운 어떤 사람이 PIN번호를 알지 못하면(카드 뒤에 PIN 번호를 작성하면 위험할 수 있음) 돈을 인출할 수 없다. 마찬가지로 PIN 번호만 알고 있다고 하더라도, 카드가 없으면 돈을 인출할 수 없다 공격자는 ATM 계정을 해킹하기 위해서는 2가지 다 필요하다. 이로 인해 2단계 인증은 훨씬 안전한 방법이다. 즉 2단계 보안 계층을 제공한다.

가능하면 2단계 인증을 사용하십시요. 우리의 정보를 보호할 수 있는 가장 강력한 방법 중 하나입니다.

2단계 인증 사용하기

2단계 인증은 각각의 계정에 대해서 개별적으로 설정해야 한다. 많은 온라인 서비스에서 2단계 인증을 제공하고 있다. 이중 2단계 인증을 하는 선도 기업은 구글이다. 구글은 전세계 수백만 명의 사람들에게 무료 온라인 서비스를 제공하기 때문에 구글 계정은 사이버 공격자의 주요 공격대상이다. 그래서 구글은 강력한 인증을 제공하는 것이 필요하였으며, 구글은 대부분의 온라인 서비스에 2중 인증을 시작한 선도 기업 중 하나가 되었다. 구글의 2중 인증 동작 방법을 이해하면 트위터, 페이스북, 애플, 인스타그램 및 많은 은행 등 대부분의 사이트에서 2중 인증 동작 방법을 이해할 수 있다.

구글의 2단계 인증은 다음과 같이 동작한다. 먼저 구글 계정에서 2단계 인증을 활성화하고, 핸드폰 번호를 등록한다. 이것이 완료되면, 2단계인증을 다음과 같이 동작합니다. 먼저 사용자명과 패스워드를 통해 계정으로 로그인 한다. 이것은 우리가 알고 있는 것에 해당하는 첫 번째 요소이다. 하지만 구글은 그 다음 우리가 가지고 있는 것인 스마트폰으로 6자리 숫자 코드를 문자 메시지로 전송한다. 패스워드와 마찬가지로, 이 번호를 입력해야 한다. 계정으로 로그인하기 위해서는 패스워드를 알고 있어야 하고, 문자 코드를 받기 위해서 핸드폰을 가지고 있어야 한다. 공격자 패스워드를 알고 있더라도, 핸드폰을 가지고 있지 않다면 구글 계정에 접근할 수 없다. 계정의 보안을 위해, 구글에서 계정이 로그인할 때마다 새로운 코드를 보내준다.

2단계 인증

구글 등 많은 사이트에서 2단계 인증을 위한 다른 방법도 제공한다. SMS 문자메시지를 받는 대신, 스마트폰에 인증 앱을 설치할 수 있습니다. 이 앱에서 로그인할 때마다 유일한 코드를 생성한다. 모바일 앱 사용하는 이점은 코드를 받기 위해 통신에 연결되어 있을 필요가 없다는 점이다. 스마트폰에서 자체적으로 코드를 생성해 준다. 추가로 이 코드는 전송되는 것이 아니라 핸드폰에서 생성되기 때문에 가로챌 수 없다.

2중 인증은 디폴트로 활성화되어 있지 않다. 이 기능을 사용하려면 사용자가 활성화해야 한다. 가능하다면 특히 이메일, 온라인 뱅킹, 파일 저장소과 같은 중요한 서비스의 경우2중 인증을 사용할 것을 강력히 추천한다. 2단계 인증은 단순한 패스워드보다 정보 보호기능이 뛰어나다.

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:	http://www.securingthehuman.org/ouch/2015#april2015
2단계 인증을 사용할 수 있는 곳:	https://twofactorauth.org
Stop|Think|Connect:	http://stopthinkconnect.org/2stepsahead
구글 2단계 인증:	http://www.google.com/landing/2step/
SANS 보안일일팁:	http://www.sans.org/tip_of_the_day.php

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