OUCH! | 2014 년 11월호

컴퓨터 사용자를 위한 월간 정보보호 인식 뉴스레터

OUCH!

이달 호 주제..

- 사회공학 공격
- 사회공학 공격 탐지 및 차단
- 미래의 공격 예방법

사회공학 공격

개요

사람들이 일반적으로 사이버공격자들은 첨단 해킹 도구와 기술을 이용해서 사람들의 컴퓨터, 계정 및 모바일 기기를 해킹한다고 오해하고 있다. 하지만 이것은 사실이 아니다. 사이버 공격자들이 정보를 훔치고 컴퓨터를 해킹하는 가장 쉬운 방법 중 하나가, 사람들에게 말로 속이는 것이라는 것을 알게되었다. 이번 달호는 사회공학적 공격이라고 하는 사람에 대한 공격의 종류와 이러한 공격으로부터 우리를 보호할 수 있는 방법에 대해서 배우게 된다.

객원 편집자

알리사 토레스는 SANS 공인강사이며, 고급 컴퓨터 포렌식 및 사고 대응과정을 담당한다. 알리사는 사고대응전문가로 최전선에서 근무하였으며, 디지털 포렌식 조사관으로서 내부 보안팀에서 일하였다. 알리사의 트위터는 @sibertor 이며, 여기서 추가정보를 얻을 수 있다.

사회공학 공격

사회공학은 공격자들이 사람들을 속여 자신들이 원하는 방향으로 움직이게 하는 심리적 공격이다. 사회공학은 수 천년 동안 존재해왔으며 사람을 속이는 생각은 새로운 것이 아니다. 하지만 사이버 공격자들은 인터넷에서 이 기법을 사용하는 것이 굉장히 효과적이며, 이를 이용하여 수 백만 명의 사람들을 대상으로 할 수 있다. 사회공학이 동작하는 방법을 가장 쉽게 이해할 수 있는 방법은 실제 세계의 사례를 보는 것이다.

우리가 컴퓨터 지원회사 또는 통신사, 마이크로소프트의 기술지원팀이라고 하는 사람들로부터 전화를 받는다. 전화한 사람은 우리 컴퓨터가 인터넷을 스캐닝하고, 스팸을 발송하는 등 이상한 행동을 보이며 감염된 것 같다고 알려준다. 이 사람들은 문제를 조사해야 한다고 하고, 컴퓨터를 확보한다. 이 사람들은 다양한 용어를 사용해서 컴퓨터가 감염된 것 같이 믿도록 만든다.

예를 들어서 이 사람들은 컴퓨터에 어떤 파일을 확인하도록 하고, 파일을 찾도록 한다. 우리들이 그 파일을 찾으면, 이 사람들은 이 파일은 컴퓨터가 감염되었다는 표시라고 믿게 한다. 그런데 실제로는 이 파일은 모든 컴퓨터에 발견되는 일반적인 시스템 파일일 뿐이다. 일단 이 사람들이 우리를 속여서 컴퓨터가 감염되었다고 믿게 만들면, 웹 사이트로 가서 보안 소프트웨어를 구매하도록 유도하거나, 컴퓨터를 수리할 수 있도록 컴퓨터에 원격 접속을 할 수 있도록 해달라고

사회공학 공격

요청한다. 하지만 판매하는 소프트웨어는 실제로는 악성 프로그램이다. 만약에 이것을 실제 구매해서 설치하면, 실제로 컴퓨터를 감염시키고, 돈도 지불해야 한다. 만약에 우리들이 컴퓨터 수리를 위해서 원격 접속을 허가하면, 실제로는 컴퓨터에 접속하여 컴퓨터를 감염시킨다.

이와 같은 사회공학 공격은 전화에 한정되어 있지 않으며, 이메일, SMS, 페이스북 메시지, 트위터 게시글 또는 온라인 채팅 등 다양한 기술로도 가능하다. 핵심은 뭘 조심해야 하는 것인지를 아는 것이다.

사회공학 공격을 예방, 탐지 및 차단할 수 있는 방법을 알면, 가장 효과적으로 우리 자신을 보호할 수 있다.

사회공학 공격 탐지 및 차단

사회공학 공격을 방어할 수 있는 가장 간단한 방법은 상식적으로 판단하는 것이다. 의심스럽고, 적절한 것 같지 않으면 공격일 수 있다. 사회공학 공격의 일반적인 지표는 다음과 같다;

- 엄청나게 긴급한 일이라고 하는 사람. 누가 빨리 결정하라고 하면 의심하라.
- 다른 사람이 접근할 수 없거나, 이미 알고 있는 정보를 요청하는 사람
- 진짜라고 믿기에는 너무 좋은 것. 예를 들어 복권을 사지도 않았는데 우리가 복권에 당첨되었다는 것

어떤 사람이 우리들을 사회공학 공격의 피해자로 만들려고 하는 것으로 의심되면, 더 이상 그 사람과 의사소통하면 안된다. 만약에 어떤 사람이 전화를 하면 끊어야 한다. 만약에 온라인으로 채팅하고 있는 사람이면, 연결을 차단해야 한다. 신뢰할 수 없는 이메일이라면 삭제해야 한다. 사회공학 공격이 업무와 관련된 것이라면, 회사의 정보보호팀에 보고해야 한다.

사회공학 공격 예방

다행히도 향후 사회공학 공격에 노출되지 않기 위한 예방법이 있다.

- **패스워드 절대 공유 금지**: 어떤 기관에서도 패스워드를 물어보기 위해 연락하지 않는다. 만약에 패스워드를 누군가 물어보면 이것은 공격이다.

사회공학 공격

- **너무 많은 것을 공유하지 마라**: 공격자가 우리에 대해서 더 많이 알수록, 자신들이 원하는 것을 할 수 있도록 우리를 속이기 쉽다. 우리 자신에 대해서 조금씩이라도 자주 공유하면 우리에 대해서 전체를 알 수 있다. SNS 사이트, 상품 평 또는 공개 포럼, 메일 리스트 등에 더 적게 공유할수록, 공격받을 확률도 낮아진다.

- **연락처 확인**: 은행, 신용카드사, 통신사 등 합법적인 이유로 전화를 받게 되는 경우가 있다. 만약에 요청하는 정보가 합법적인지 의심스러우면, 상대방의 이름과 전화번호를 물어봐야 한다. 그리고 신용카드 뒷면의 전화번호, 은행 고지서에 있는 전화번호 또는 회사의 웹사이트에 있는 전화번호와 비교해서 맞는 지 확인해야 한다. 이렇게 우리가 직접 기관에 전화할 때 우리가 실제 기대하는 사람과 통화할 수 있다. 귀찮을 수 도 있지만, 우리의 신분과 정보를 보호하는 것이 더 중요하기 때문이다.

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
소셜 네트워킹 안전하게 사용하기:	http://www.securingthehuman.org/ouch/2013#march2013
사기 예방:	http://www.onguardonline.gov/topics/avoid-scams

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