정 보 보 호 학 회 지
제25권 제4호, 2015. 8

인간의 감정 상태를 이용한 사회공학 기법 연구

박 재 혁*, 이 재 우**

요 약

최근의 정보보호 관련 사고를 살펴보면 기업 내부자로 인한 개인정보의 유출과 같이 특별한 기술 없이 이루어지는 인간 중심의 정보보호가 이슈화되고 있다. 그만큼 점점 사회공학적인 위협이 증가하고 있는 추세이며, 그 위험성이 사회 전반적으로 인식되어가고 있다. 본 지를 통해 사회공학의 의미에 대해 되짚어보고, 사회공학 라이프 사이클과 최근의 사회공학 공격 기법에 대해 분석한다. 또한 일반적 사회공학 의미인 인간 상호 작용의 깊은 신뢰를 바탕으로 사람들을 속여서 보안 절차를 우회하는 등의 기존 개념에 더하여 유사한 사례를 바탕으로 인간의 대표적 감정 상태(두려움, 슬픔, 기쁨)를 이용한 사회공학 기법에 대해 논한다.

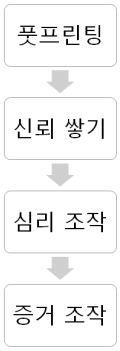
Ⅰ. 서 론

사회공학(Social Engineering)은 컴퓨터 보안에서 인간 상호 작용의 깊은 신뢰를 바탕으로 사람들을 속여 정상 보안 절차를 깨트리기 위한 비기술적 침입 수단이라 정의할 수 있다. 우선 정보통신망에서 보안 정보에 접근 권한이 있는 담당자와 신뢰를 쌓고 이메일이나 전화 등을 통해 그들의 약점을 이용하는 것이다. 상대방의 자만심이나 권한을 이용하는 것, 정보의 가치를 몰라서 보안을 소홀히 하는 무능에 의존하는 것과 도청 등이 일반적인 사회공학 기술이다. 이 수단을 이용하여 시스템 접근 권한와 패스워드를 알아내 시스템에 침입하는 것으로 네트워크 및 시스템 보안 못지않게 사람 중심의 정보보호가 중요시 되고 있다. 사회공학의 대표격인 ‘Kevin Mitnik’의 말에 의하면, “기업 정보보안에 있어서 가장 큰 위협은 컴퓨터 바이러스, 패치가 적용되지 않은 중요한 프로그램이나 잘못 설정된 방화벽이 아니다. 가장 큰 위협은 바로 당신이다.” 라고 정의한다. 그만큼 정보보호에 있어서 가장 취약하고 위험한 위협원은 사람이다.

본 지에서는 사회공학을 일으키는 요인과 사례를 통해 인간의 감정 상태에 따른 사회공학 기법에 대해서 연구한다.

Ⅱ. 사회공학 라이프 사이클

사회공학 공격은, 아래의 그림 1과 같은 사회공학 라이프 사이클을 통해서 이루어진다.



〔그림 1〕 사회공학 라이프 사이클

2.1. 풋 프린팅(Footprinting)

풋 프린팅은 목표 대상 및 주변 환경에 대한 정보를 축적하고, 성공적인 공격의 가능성을 개선하도록 목표 대상과 좋은 관계를 형성하는 과정이다. 풋 프린팅을 하는 과정에서 다음과 같은 사항들이 포함된다. 이름, 휴대폰번호, 직위, 학력, 위치 정보 등 실제 사회공학 공격을 시작하기 전에 공격 대상에 대한 정보를 미리

* 동국대학교 국제정보대학원 정보보호학과(pjhw119@naver.com)
** 동국대학교 국제정보대학원 정보보호학과 석좌교수(jwlee0904@paran.com)

수집한다.

2.2. 신뢰 쌓기

공격자는 공격 대상에게 좋은 관계를 형성하기 시작하고, 이후에 피해자는 공격자가 요청한 정보를 공개할 가능성이 높아진다. 사회공학 공격자는 얻은 신뢰를 바탕으로 신분을 사칭하거나 피해자에게 얻은 내부 정보를 통하여 비즈니스에 심각한 영향을 미칠 수 있는 기밀도가 높은 정보들을 수집한다.

2.3. 심리 조작

사회공학 공격자는 좀 더 쉽게 공격 대상에 접근할 수 있게 공격 대상에 대한 민감한 정보를 모아 기밀정보를 추출하거나 추론할 수 있도록 이전 단계에서 얻은 신뢰를 바탕으로 피해자의 심리를 조작한다.

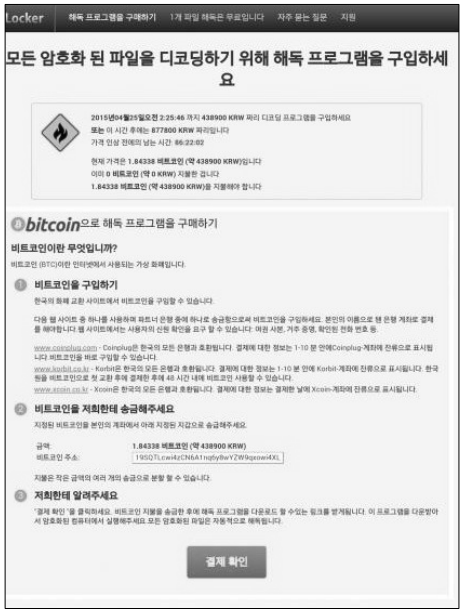
2.4. 증거 조작

위의 단계를 거쳐 얻은 기밀성 있는 자료들을 얻은 후에, 사회공학 공격자는 자신에게 불필요한 의심을 품지 않게끔 명확하게 증거를 조작한다. 사회공학 공격자는 자신의 정체를 드러내지 않도록 역 추적에 대한 대비와 증거를 정리하고 마무리 한다.

Ⅲ. 최근의 사회공학 기법

3.1. 랜섬웨어(Ransomeware)

랜섬웨어는 ransom(몸값)과 ware(제품)의 합성어로 컴퓨터 사용자의 문서를 인질로 잡고 돈을 요구한다고 해서 붙여진 명칭이다. 랜섬웨어에 감염될 경우 파일이 복잡한 알고리즘으로 암호화 돼 파일을 열어도 내용을 알아 볼 수 없다. 주로 이메일, 소셜네트워크서비스(SNS), 메신저 등을 통해 전송된 첨부파일을 실행하면 감염되며, 웹사이트 방문을 통해 감염되기도 한다. 백신 프로그램으로 악성코드를 없애도 암호화된 파일은 복구되지 않아 사상 최악의 악성코드라고 불린다. 해커들은 파일을 열 수 있게 해준다는 조건으로 돈을 요구하는데, 기한이 지나면 액수가 더 증가하고 파



〔그림 2〕 한국형 랜섬웨어 크립토락커

일을 복구할 수 없게 할 수 있다고 협박하기도 한다. 처음 러시아에서 유행하면서 랜섬웨어를 이용한 사기는 국제적으로 증가하였는데, 보안 소프트웨어 개발사 맥아피는 2013년 1분기 동안 수집한 250,000개 이상의 독특한 랜섬웨어 샘플 자료를 2013년 6월 공개했고, 이는 2012년 1분기보다 두 배 많은 수치였다. 2013년 말 발견된 랜섬웨어 바이러스인 크립토락커는 미국 당국에 의한 색출을 당하기 전까지 미화 약 300만 달러를 갈취했다.

보통 인터넷 사용자의 컴퓨터에 잠입해 내부 문서나 스프레드시트, 그림파일 등을 암호화해 열지 못하도록 만든 후 돈을 보내주면 해독용 열쇠 프로그램을 전송해 준다며 금품을 요구하는 악성 프로그램이다. 최근에는 그림 2와 같이 국내에서 랜섬웨어의 일종인 크립토락커 한국어 버전이 국내 웹사이트에서 유포되고 있어서 감염된 PC 시스템 파일을 제외한 마이크로소프트(MS) 오피스 문서 파일, 한글문서 파일, 압축 파일, 동영상·사진 등을 무단으로 암호화한 후 해독 조건으로 96시간 내 돈을 지불하도록 유도했다. 공격자는 익명 네트워크인 토르(Tor)를 사용하는 동시에 가상화폐 비트코인으로 돈을 지불하도록 하는 등 추적을 어렵게 하는 치밀함을 보였다.

3.2. 웨일링(Whaling)

웨일링은 고래를 잡는다는 표현과 같이 기존의 피싱 공격과 다르게 고위 경영진이나 지도자들을 대상으로 한 피싱이라고 할 수 있다. 사회공학 공격자는 무역 또는 군사 기밀, 금융 정보 등의 이익을 위해서 피싱과 비슷한 방법으로 피해자에게 피해를 입힌다. 웨일링은 이메일에 첨부된 파일을 다운로드하거나 링크를 클릭하는 행동으로 시작되는데 공격자는 고위 경영진 등의 권한으로 접근하여 원격으로 컴퓨터를 제어하거나 키 입력을 기록 받을 수 있다. 링크를 클릭하게 되면 문서나 서비스, 소프트웨어들을 다운로드 하여 접근하려면 자격 증명을 입력하게끔 하거나 금융 정보를 입력해야만 한다는 메시지를 파밍 사이트로 이동시키게 한다. 파밍된 조작된 사이트에서 고위 경영진 등이 정보를 입력하면 이를 통해 조직의 중요한 기밀 정보가 유출되거나 금전적인 손실이 발생하게 된다.

3.3. 역 사회공학(Reverse Social Engineering)

역 사회공학은 사회공학에서의 사회공학이라고도 할 수 있으며, 자동화된 사회공학 공격 방법이라고도 할 수 있다. 이 공격은 공격자가 반대로 피해자가 될 수 있는 공격이기도 하고, 피해자가 의도치 않게 공격자로 전환될 수 있는 특이한 형태의 사회공학이라 할 수 있다. 공격자는 1단계로 희생자의 호기심을 자극하여 미끼 형태로 중간에서 피해자를 기다린다. 2단계로 공격자는 미끼에 최초로 접근하는 피해자를 기다리고 피해자들을 끌어 모으기 위해 피해자들에게 사회공학을 한다.

역 사회공학에서는 공격자가 직접 공격을 수행하는 것이 아닌 다소 정보보호에 대한 지식이 부족하거나 의식이 부족한 업무 담당자가 문제가 있는 스팸 메일을 수신하거나 특정 사이트의 주소를 클릭하도록 유도하는 공격으로부터 시작한다. 자동화 사회공학은 공격을 당하는 희생자가 이메일 문자 및 사이트 클릭 등을 통해 공격당하기 때문에 역 사회공학이라고 불린다. 특히나 근래에는 소셜네트워크서비스를 많이 이용하게 되면서 페이스북과 같은 서비스에서 친구 관계로 인해 역 사회공학 취약점이 쉽게 노출되곤 한다. 많은 친구들이 유명 인사의 페이스북 페이지 링크를 클릭하면,

〔그림 3〕 소셜네트워크 서비스 페이스북

메시지 수신 및 댓글 달기 등이 순조롭기 때문에 역 사회공학으로 인한 공격에 쉽게 감염된다.

예를 들어, 갑이 악성스크립트가 작성된 게시물에 을을 태그하게 되고 이를 통해 을은 자동적으로 악성스크립트를 포함한 게시물의 소유자이면서 작성자가 된다. 이후에 악성스크립트가 작성된 게시물은 자동적으로 을의 친구 목록에 있는 친구들을 모두 태그로 불러들여서 을은 의도치 않은 공격자가 되고 또한 을의 친구들 또한 의도치 않은 피해자이면서 공격자가 되는 피라미드 구조의 사회공학 공격 형태가 된다. 그러므로 정상 사용자가 역 사회공학 기반 공격자와 친구로 맺어지면 보안에 취약한 이메일이나 쪽지 문자 및 사이트 댓글 등도 수락하거나 클릭하기 쉽다. 이는 소셜네트워크서비스인 페이스북에서 가장 유효하게 수행될 수 있는 사회공학 공격 기법이다. 게시물의 작성자가 게시물을 작성하게 되면 그림 3과 같은 형태로 게시물이 등록되게 된다. 이 후에 작성자와 친구 관계인 다른 사람들이 이 게시물에 덧글을 작성하거나 친구 관계인 사람들의 친구들을 이 게시물에 태그하여 게시물을 열람할 수 있게끔 한다. 하지만, 만일 최초 게시물 작성자가 코드 은닉 형태의 기법으로 악성 스크립트가 작성된 게시물을 작성하였다면, 이후에 이 게시물에 댓글을 작성하거나 친구들을 태그하게 되면 이 후에는 자동으로 이 게시물에 관련된 사람들은 모두 피해자이면서 가해자가 되는 특이한 형태로 사회공학 공격이 진행된다.

Ⅳ. 인간의 감정 상태를 이용한 사회공학 기법

인간의 감정 상태에서 대표적인 감정인 두려움, 기쁨, 슬픔에 대한 분석과 인간의 감정을 이용한 사회공학 기법에 대하여 연구한다. 인간의 감정의 표현에 대한 분석은 심리학자 '폴 에크먼'의 이론에 기초하며, 미세표정(Microexpression)을 통한 인간의 감정 표현이 어떠한 방법으로 표출되는지 분석한다. 또한 이러한 인간의 감정이 어떻게 사회공학적으로 악용되는지 분석하고, 인간의 감정 상태에 따른 사회공학 기법 사례에서는 갑을 사회공학 피해자로, 을을 사회공학 공격자로 구성하여 이메일 피싱과 파밍 공격 기법을 바탕으로 분석한다.

4.1. 두려움

두려움은 공포(恐怖)와도 유사한 의미의 감정이고, 두려움의 사전적인 의미로는 두려운 느낌과 무서워하는 감정이라고 할 수 있다. 두려움의 감정은 생후 5~7개월이 지나면 점점 느끼게 되며, 보통 두려움의 시작은 높은 곳에 올라와 있을 때나 천둥소리와 같은 큰 소리에서부터 시작이 된다. 이러한 두려움의 감정은 대부분 학습에 의해서 이루어진 것이며, 경험에 의해서 이루어진 감정이라 할 수 있다. 두려움의 심리적 상태는 놀라움과 두려움이 얼굴에 유사한 근육의 움직임을 통해서 두 감정이 혼동될 수 있다. 두려움과 놀람은 보통 같이 느끼는 경우가 많으며 놀랐을 때도 두려움과 마찬가지로 눈썹이 올라가고 눈이 커지지만, 입술의 가장자리가 아래로 쳐지면서 아래턱의 피부가 아래로 움직이는 것은 두려움을 느끼는 것이다.[2]

두려움의 감정은 사회공학의 관점에서 사람들이 특정한 반응을 하게끔 하는데 사용되곤 한다. 두려움을 이용하는 사회공학 공격자는 인터넷 사이트의 배너를 클릭하거나 정보의 중요한 부분을 포기하는 등 순진한 사용자를 속이기 위해 공격을 시도한다. 예를 들어 이 악성 배너는 컴퓨터가 바이러스에 감염되어 시스템이 손상될 수 있다는 등의 방법으로 사용자로 하여금 두려움을 유도하게 만든다. 특히나 이 두려움을 이용하는 사회공학 공격자는 컴퓨터 기술에 많은 지식이 없는 사용자에게 매우 유효한 심리적 공격 방법이다.

그렇다면 이러한 인간의 두려움의 감정을 이용하는 사회공학 기법의 예시에 대해서 알아보도록 하겠다. 과거에 갑은 대형 유통마트에서 진행하는 상금 이벤트에 응모한 경험이 있고, 이벤트 결과는 응모 시 제출한 이메일로 결과를 통보를 받게 되어있다. 사회공학 공격자인 을은 피해자인 갑의 이메일 주소를 획득한 후에 이메일 피싱을 시도한다. 공격자인 을이 1억원의 상금을 수령하라 갑에게 이메일을 보내게 되면, 갑은 이에 대해서 의구심을 품을 수 있지만 우선 이메일 내용을 수용할 것이다. 그러나, 차후에 을이 갑에게 이메일로 1억원의 상금을 받고 싶으면 50만원 상당의 예치금을 입금하라는 메시지와 함께 입금 계좌 번호를 첨부하여 발송하였다. 만일 예치금을 입금하지 않으면 이 상금은 다음 순위 응모자에게 차례가 넘어감을 주의사항에 작성하여 갑에게 전달한다. 갑은 상금을 수령하려면 예치금이 필요하다는 사실을 인지함과 동시에 예치금을 입금하지 못하면 1억원의 상금을 잃을 수 있다는 두려움에 휩싸이게 될 것이다. 갑은 무언가 의문점이 있다고 생각하지만, 1억원의 상금의 기회를 다음 사람에게 넘겨주어야 한다는 두려움에 이메일에 첨부된 계좌번호로 50만원의 예치금을 입금하게 된다. 그러나 이는 인간의 두려움을 이용한 사회공학 공격에 피해를 입은 것으로, 결국 갑은 1억원의 상금을 수령하지 못하고 50만원의 금융사기를 당하게 된다.

4.2. 기쁨

인간의 감정에서 기쁨을 느끼기 위해서는 무언가를 자신이 쟁취하거나 얻었을 때에 그 감정이 발생할 수 있는데, 이는 인간의 생존에 직결되는 도움이라 할 수 있다. 예를 들자면, 맛있는 음식을 먹는다든가, 자신이 원하는 시험에 합격을 하는 등의 즐거운 상황이다. 이는 대부분 인간의 활동에 있어서 특정 행동의 보상을 해주는 일들이라 할 수 있다. 기쁨은 얼굴에 웃음으로 드러나며 웃음소리와 동반될 수 있다. 기쁨의 감정을 느끼게 되면 눈이 평상시보다 커지게 되며, 입은 열려서 귀에 닿을 것과 같이 된다. 이러한 기쁨의 상태로 인해 만족 상태가 되면 교감 신경의 흥분을 동반하기에 심장 박동 수가 빨라지게 되고 얼굴이 붉어지는 등 가슴이 벅차오른다. 이후에는 기쁨에 만족 상태가 지속되면 심장 박동 수가 감소하게 되고 고요함과 편안함을 느끼게 된다. 또한 몸짓에 있어서도 알 수가 있는데,

보통 기쁨의 감정을 느끼게 되면 두 손이 위로 올라가는 현상이 일어난다. 슬픈 상태에서는 대조적으로 두 손이 아래로 처지는 것과는 대조적인 현상이다. [2]

기쁨을 이용하는 사회공학 공격은 인터넷 사이트의 배너를 클릭하거나 정보를 통해서 좀 더 손쉽게 무언가를 쟁취할 수 있거나 별다른 행동을 하지 않아도 의도하지 않은 특유의 보상을 받게 되는 경우에 유효하다. 예를 들어 이 배너를 클릭하여 사이트에 접속해서 광고를 시청하기만 해도 사용자는 손쉽게 돈을 벌 수 있다는 식으로, 별다른 노력을 하지 않고도 사용자가 무언가를 쉽게 쟁취할 수 있다는 방식으로 사회공학 공격을 시작하게 된다.

그렇다면 이러한 인간의 기쁨의 감정을 이용하는 사회공학 공격의 예시에 대해서 알아보도록 하겠다. 과거에 갑은 상품 구매 후기 이벤트를 응모한 적이 있었고 이벤트의 1등 당첨자는 1억원 상당의 상금을 수령할 수 있음을 알고 있었다. 이 후에 사회공학 공격자인 을은 갑이 응모한 사실을 알고 갑의 이메일 주소로 이메일 피싱을 시도하였다. 공격자인 을은 상품 이벤트 회사 담당 직원으로 신분을 속여 피해자인 갑에게 “당신은 1억원의 상금을 탔으니 첨부 파일에 있는 첨부 문서에 내용을 작성하여 회신해달라는 메시지를 받게 된다. 갑은 이 과정에서 자신이 상금을 탔다는 기쁨에 휩싸여 첨부 파일에 있는 첨부 문서를 열어보았다. 그러나 첨부된 문서를 여는 과정에서 안티바이러스 프로그램을 종료하라는 알림과 함께 이 파일을 다운로드 받으면 시스템에 위협이 가해질 수 있다는 운영체제 경고 메시지를 보게 되었다. 피해자인 갑은 무언가 의문점이 생겼지만, 그보다 자신이 1억원의 상금을 탔다는 기쁨에 휩싸여 운영체제 보안 수준을 최소 수준으로 낮추고 안티 바이러스 프로그램을 종료하게 되었다. 이 후에 첨부 문서를 활성화 하는 순간 갑의 컴퓨터는 악성코드에 감염되게 되어, 공격자인 을은 갑의 컴퓨터에 원격 접근하여 중요한 기밀 정보들을 훔쳐가고 말았다. 물론 갑은 1억원의 상금을 받을 수 없었으며, 자신이 사회공학의 피해자가 되었음을 깨닫는 순간 자신의 기쁨의 감정 상태로 인해 피싱 사기를 당하게 되었음을 알게 되었다.

4.3. 슬픔

슬픔의 감정은 슬픈 마음이나 느낌으로 설명이 되고, 원통한 일을 겪거나 불쌍한 일에 마음이 괴롭다는 설명도 된다. 이러한 슬픔은 자신이 가지고 있는 소중한 사람이나 물건을 잃는다든가 시험에 떨어지게 되면 슬픔의 감정을 느끼게 된다. 보통 슬픔의 감정은 기쁨과 대조되는 감정이지만, 상호 유기적인 감정 연계가 된다. 예를 들어, 지갑을 지하철에 두고 내린 줄 알았으나, 가방에서 지갑을 발견한다면 슬픔을 미처 느끼기 전에 기쁨을 느끼게 된다. 슬픔의 감정을 알 수 있는 방법은 대부분 상대방의 얼굴을 보면 알 수 있는데, 올라간 눈썹과 양 옆으로 당겨진 입, 약간 아래로 처진 입가와 위로 올라간 양쪽 뺨이다. 슬픔의 감정을 느끼는 순간 말초 혈관이 확장되면서 얼굴이 붉어지면서 눈물이 흐르는 순간 더욱 붉어지게 된다. 또한 슬픔을 느끼게 되면 얼굴의 근력이 떨어지게 되면서 어깨가 처지고 힘이 없어지면서 목소리가 약해지면서 떨리기도 한다.[2]

슬픔을 이용하는 사회공학 공격자는 인터넷 사이트의 배너를 통해 사람들의 슬픔을 자극하는 형태의 문구나 사진 및 그림 등을 통해서 불쌍한 일에 피해자들로 하여금 마음을 괴롭게 만든다. 예를 들어 사회공학 공격자는 슬픔을 유도하는 배너를 클릭하여 사이트에 접속해서 유명한 사회복지 단체나 국제봉사 단체 등으로 위장한 파밍 사이트를 통하여 불우한 이웃들을 돕자는 형태의 게시물을 통해서 돈을 입금 받게 하는 등의 형태로, 슬픔을 느끼는 사람들로 하여금 각종 사기 피해를 입게 한다.

그렇다면 이러한 인간의 슬픔의 감정을 이용하는 사회공학 공격의 예시에 대해서 알아보도록 하겠다. 갑은 평소에 불우이웃을 돕는데 자신의 수입의 일부를 자주 불우이웃 돕기 단체에 기부를 한다. 갑은 컴퓨터에 대한 지식이 깊지 못하여, 보통 불우이웃 돕기 성금을 기부하는 데에 오프라인 기부 방식으로 기부를 해오곤 하였다. 어느 날 갑은 불우이웃 돕기 단체인 유니세프의 명의로 된 이메일을 받게 되었다. 이메일에는 불우한 전 세계의 이웃을 위해 기부를 요청하는 식의 도움을 요청하는 문구와 함께 독자의 슬픔을 유도하는 불우이웃들의 사진과 불우이웃 돕기 계좌번호가 함께 동봉되어 있었다. 갑은 이메일 내용에 대해 슬픔의 감정

을 느끼게 되어 의심의 여지없이 동봉된 계좌번호로 성금을 송금하게 되었다. 며칠 뒤에 갑은 뉴스를 통해서 이러한 형태의 사기를 주의하라는 것을 알게 되었고, 갑은 슬픔의 감정에 휩싸여 금융사기를 당하게 되었다.

이러한 사기의 배경에는 사회공학 공격자인 을이 조작한 유니세프 단체의 파밍 사이트로, 실제로 불우이웃돕기 이메일을 받은 독자들은 의심의 여지없이 기부금을 첨부된 계좌번호로 송금하게 되었던 것이다.

Ⅴ. 결 론

최근에 발생한 정보보호 사고들을 살펴보면 많은 수의 공격 기법이 인간의 취약점을 이용한 공격의 경우가 다수였다. 더불어 정보 유출 사고의 경우 대부분 내부자의 위협으로 인해 개인정보나 기업 기밀이 유출되어 기업의 존폐가 걸렸던 중대한 사건들도 있었다. 지금까지의 사회공학 공격들을 분석해보면 대다수가 조직 내부자의 정보보호 취약점과, 이에 따른 사회공학 공격 방법으로 사회공학에 대한 사회 이슈를 다루는 사례가 많았다.

본 지에서는 인간의 감정적인 취약점을 이용한 사회공학 기법에 대해서 분석하였다. 인간의 대표적인 감정인 두려움, 기쁨, 슬픔에 대하여 분석하고, 이에 따른 사회공학 기법에 대한 사례를 통해 분류하였다. 본 지에서 다룬 사회공학 사례인 이메일 피싱과 같이 동일한 사회공학 기법이라 할지라도 인간의 감정에 따라 여러 측면의 접근 방법으로 사회공학 공격이 시도됨을 알 수 있다. 향후에는 다양한 인간의 감정에 대해서 분석이 필요하고, 인간의 감정에 따른 사회공학 기법들의 새로운 분류 체계에 대한 연구가 필요할 것으로 예상된다.

참 고 문 헌

[1] Ayesha Khan, “How to deal with Social Engineering”, SANS GSEC Practical Assignment 1.4b, 2002년 12월.

[2] Christopher Hadnagy, “The Art of Human Hacking”, Wiley Publishing, Inc. 2011년.

[3] Danesh Irani 외 3명, “Reverse Social Engineering Attacks in Online Social Networks”, College of Computing, Georgia Institute of Technology, Atlanta, 2010년.

[4] Chan D Lieu, ”Social Engineering – Attacking the Weakest Link”, SANS Institute InfoSec Reading Room, 2002년.

[5] Martin Manjak, “Social Engineering Your Employees to information Security”, SANS Institute InfoSec Reading Room, 2008년.

〈저 자 약 력〉

박 재 혁 (Jae-Hyeok Park)
학생회원
2014년 2월 : 고려대학교 경영정보학과 졸업
2014년 3월~현재 : 동국대학교 정보보호학과 석사과정
관심분야 : 정보보호전략/관리, 모바일보안, E-Business 전략

이 재 우 (Jae-Woo Lee)
동국대학교 국제정보대학원 석좌교수(현)
한국포렌식조사전문가협회 회장(현)
ISC2 Fellow, Asia Board 의장(현)
한국 CSO 협회 자문위원장(현)
한국정보보호진흥원 초대 원장