"사용자 쿡쿡 찔러 '자발적'으로 '참여' 유도 하자"

넛지와 시큐리티 어웨어니스 … 능동적인 사용자 동참 유도

연재순서

1. 넛지와 시큐리티 어웨어니스(이번호)
2. 사용자 쿡쿡 찌르기(1)
3. 사용자 쿡쿡 찌르기(2)

최근 유래 없는 보안 사고들이 빈번하게 발생하며 신문 지면과 방송에 떠들썩하게 오르내리고 있다. 특히 최근의 사고는 대규모 개인정보 유출, 금융거래 중단 등 일반 국민들의 생활에 직간접적인 영향을 끼치는 것들이었기에 그 어느 때보다 일반 대중의 보안에 대한 경각심과 관심을 높이고 있다.

매번 대형 사고들이 발생하면 대부분의 IT보안 전문가들은 '기업과 기관의 사용자 보안의식을 높여야 한다'는 것을 해결책으로 제시하지만 사용자의 '보안의식' 부재 해결이 보안 사고를 예방할 수 있는 최선의 선택이지만, 어떻게 하면 보안의식을 높일 수 있는지 실천적인 방법들에 대한 접근과 논의는 상당히 부족하다. 앞으로 3회에 걸친 연재를 통해 조직의 보안의식 수준을 어떻게 하면 높일 수 있는지 실천적이고 구체적인 아이디어를 함께 고민해 보자.

'사람'은 정보보호에 있어서 가장 취약한 연결고리로 언급되곤 한다. 고의적인 것이든 우발적 실수에 기인한 것이든 상관없이 사람은 네트워크와 IT 인프라에서 가장 취약한 지점이다. 커다란 쇠사슬의 강도는 평균 두께와 강도가 아닌 가장 약한 고리에 의해 결정된다. 가장 약한 부위가 표적이 되어 공격을 당하면 커다란 쇠사슬일지라도 쉽게 끊어질 수밖에 없다.

가장 취약한 연결고리 '사람'

최근 대규모 해킹 피해를 입은 SK커뮤니케이션즈나 농협 또한 보안에 지속적인 투자를 하고 최첨단 보안 솔루션을 구축/운영하고 있는 기업들이었다. 방화벽, 침입탐지시스템 및 악성코드 탐지 솔루션 등 다양한 첨단 보안장비를 갖춘 곳이었음에도 당한 이유는 무엇일까? 외부의 공격자가 조직의 IT 인프라에 침투하기 위해 가장 취약한 연결고리를 노리고, 이를 집중적으로 파고들었기 때문이다.

물리학자 출신의 앨리 골드랫 박사는 '제약이론(TOC: Theory of Constraints)'에서 "모든 기업은 보다 높은 수준의 성과를 얻어낼 수 없도록 성과를 제약하는 자원이 반드시 하나 이상 존재한다. 기업은 이러한 제약 자원을 파악하고, 개선해야만 기업의 성과를 향상 시킬 수 있다"고 말한다.

최근 대형 개인정보 유출사고가 잇따르면서 보안에 대한 경각심이 높아지고 있다. 보안 해결책으로 제시되는 것 중 하나가 사용자 인식 강화이지만, 이는 말처럼 쉽게 이뤄지는 일은 아니다. '사람'은 보안의 출발점인 동시에 종착역으로 매번 사용자의 보안 인식 강화가 강조되지만 실제로 이뤄지지는 않고 있다고 보인다. 실질적인 사용자 인식 강화를 꾀할 수 있는 방안을 알아본다. 〈편집자〉

이동범 지니네트웍스 대표이사 / dblee@geninetworks.com

이 제약이론은 기업의 IT보안에 적용할 수 있다. 기업이 높은 보안수준을 유지하려면 보안을 제약하는 자원을 개선해야 하는데, 그 보안수준을 제약하는 자원은 바로 사람이 된다.

우리는 보안에 대해서 너무 기술 위주의 접근만을 하고 있으며, 사람에 대한 부분은 도외시하거나 무시하는 경향이 많다. 장비와 솔루션에 많은 투자를 했을지라도 내부 사용자와 관련한 취약성을 계속 방치한다면 사고는 언젠가 발생하게 될 것이고, 보안에 대한 투자는 자금만 낭비하게 되는 꼴이 될 수도 있다.

넛지(nudge)란?

작년에 '넛지(nudge)'라는 제목을 가진 책이 대형서점과 온라인상의 베스트셀러로 선정되며, 많은 사람들에게 알려졌다. 사전적 의미에서의 넛지(nudge)는 '팔꿈치로 슬쩍 찌르다'라는 뜻이다. 이것을 사회행동학적으로 적용하면 '타인의 행동을 유도하는 부드러운 개입'이며, 좀 더 적극적으로 해석하면 '타인의 똑똑한 선택을 유도하는 선택 설계의 틀'이라 할 수 있다.

넛지의 가장 재미있는 예는 암스테르담 스키폴 공항의 남자 화장실 소변기다. 보통 남자 화장실 소변기 주변은 오조준(?)으로 청결하지 못한 경우가 많다. '남자가 흘리지 말아야 할 것은 눈물만이 아니다'라는 재미있는 안내문은 이제는 별로 큰 효과를 발휘하지 못하고 있다.


▲ 스키폴 공항의 소변기

스키폴 공항의 넛지식 해결 방법은 소변기에 파리 스티커를 붙이는 것이었다. 볼 일을 볼 때 파리라는 조준점에 집중하는 남자의 심리를 이용, 실제로 화장실 환경을 경이롭게 개선할 수 있었다고 한다. 참여자들을 귀찮게 한다거나 인내심을 요구하지 않으면서도 효과적인 개선을 이루는 것이 넛지를 활용한 습관 개선의 포인트이다. 게다가 파리 스티커 제작에 큰 돈이 들어가지도 않았으니 그야말로 좋지 아니한가?!

넛지를 설명할 때 자주 등장하는 주인공 중 하나가 코끼리다. 많고 많은 동물 가운데 어째서 코끼리인 것일까? 커다란 덩치의 코끼리는 기수 한 사람의 힘으로는 제압할 수 없는 까닭이다.

채찍이나 창을 이용해 원하는 방향으로 이끌 수는 있겠지만 이런 것들은 매우 단기적인 방법이라 그 효과가 오래가지 않는다. 어쨌든 기수는 코끼리가 자발적으로 기수가 원하는 방향으로 진행시켜야 하는데, 이때 필요한 것이 넛지식 방법이다.

이것을 오늘날 IT 보안에 대입해보면, 기업 보안 관리자는 코끼리 기수이고 일반 사용자들은 코끼리라고 할 수 있겠다. 한 사람의 담당자나 한정된 인원이 다수의 사용자들을 물리적인 힘만으로 끌고 가는 데에는 한계가 있다. 기업의 팍팍한 보안규정과 사규를 들먹거리며 강제하는 것은 코끼리를 채찍과 창으로 찔러대는 것과 동일하다. 반발하거나 죽는 코끼리가 나올 수도 있고, 기수도 크게 다칠 수 있다.

얼마 전에 인터넷 상에서 '00전자를 떠나는 연구원이 CEO에게 남긴 글'이 화제가 됐다. 대기업들이 입버릇처럼 혁신을 떠들어 대지만, 실제적으로는 혁신에 역행하는 조직문화에 대해 비판하는 내용이었다. 이 글에서 연구원은 회사의 지나친 보안정책에 불만을 나타냈다.

회사가 보안이라는 이유로 특정 사이트에 대한 접근을 차단하면서 이에 대한 공지도 없었고 이유 또한 알려주지 않았다. 이처럼 무조건 따르라는 식의 보안은 구성원들의 공감을 이끌어 내기 어렵고 반발하게 만들 수도 있다. 하지만 대부분의 기업과 기관이 구성원들에게 이러한 보안을 강요하고 있다.

보안을 업(業)으로 하고 있는 필자는, 이 내용을 읽으면서 다시 한 번 생각하게 됐다. 왜 기업의 보안 관리자가 힘든지, 사용자들을 강제로 끌고 갈 때 어떤 부작용이 있는지, 효과적으로 사용자들을 참여하게 하는 왜 필요한지에 대해 말이다.

실제로 현장의 보안 관리자들은 매우 곤경에 처해 있다. 날로 첨예화되는 기술을 펼치는 해커들은 대상을 넓혀가며 공격하고 있고, 혹시라도 사고가 나게 되면 각종 규제와 법률에 따른 민 · 형사상의 처벌이 더 강화되고 있다. 또한 보안이 중요하다고 너도 나도 떠들어 대고는 있지만, 실제로 예산과 인력 지원은 미비해 일반 사용자들은 보안팀이나 보안 관리자에게 그리 우호적이지 않다. 이러한 상황은 실무팀의 고민을 날로 늘게 할 수밖에 없게 만든다.

이러한 고민을 한 방의 솔루션으로 해결할 수는 없다. 하지만 더 나은, 더 효과적인 개선안은 필요하며, 이를 위해 넛지식 풀이가 요구된다.

Knowing과 Awareness의 차이

우리말로 '인식(認識)'과 '인지(認知)'는 뜻을 명확히 구별하기 힘들어 혼용돼 사용되는 경우가 많다. 지(知)가 두뇌의 기억 영역에 국한된다면, 식(識)은 두뇌의 기억 영역과 가치 및 행동판단 영역까지 포함하고 있다고 할 수 있다. 인지(認知)는 'Knowing', 인식(認識)은 'Awareness'이다.

조직 구성원, 즉 사용자들에게 필요한 것은 보안에 대한 인지(knowing)가 아니라 보안에 대한 인식(Awareness)이다. 대부분의 사람들은 '의심스러운 첨부파일을 열면 안 된다'라는 것을 이미 알고(Knowing) 있다. 하지만 그 첨부된 파일이 의심스러운 파일인지 아닌지를 정확하게 분별해내는 것은 어떨까? 이것은 단순한 알아서(Knowing) 할 수 있는 게 아니라 정확한 인식(Awareness)이 있어야 가능하다.

보안 강의를 하면서 청중들에게 "MS 오피스에서 파일을 저장할 때 암호화 기능을 제공하는 '사실'을 아시는 분 계신가요?"하고 물으면 70~80%의 사람들이 알고 있다고 손을 든다. 그런데 "MS 오피스에서 어떤 메뉴를 선택해서 들어가야 암호 저장을 할 수 있는지 아는 분 계신가요?"라며 질문하면 대부분 손을 들지 못한다. 이것이 단순한 앎(Knowing)과 명확한 인식(Awareness)의 차이점이다.

시큐리티 어웨어너스 전략의 기본

본격적으로 넛지를 이용한 사용자 보안의식 강화 방법을 소개하기에 앞서 보안인식(Security Awareness) 강화 프로그램과 관련된 몇 가지 기본적인 가이드라인을 소개하고자 한다.

1. 기본적으로 사람과 관련된 보안 취약점은 완벽하게 제거할 수 없음을 인정한다.

그럼에도 불구하고 잘 설계된 보안인식(Security Awareness) 강화 프로그램은 적절한 수준에서 위험을 급격하게 줄이는데 큰 도움이 될 수 있다는 확신을 가져야 한다.

2. 사용자의 적극적인 피드백(feed-back)을 받을 수 있도록 프로그램을 설계한다.

이 프로그램의 핵심은 사용자에게 정보 자산을 지키는 일이 IT 관련 팀의 업무로만 여기는 것이 아니라, 자신의 정보 자산은 자신이 지켜야 한다는 것을 일깨우는 것이 가장 큰 목표다. 따라서 일반 사용자의 피드백을 중요하게 여겨야 한다. 아무리 좋은 아이디어와 방법론이라고 하더라도, 보안 관리자에게 일방적으로 끌려간다고 느끼는 순간, 사용자들은 보안업무는 똑똑한 당신의 몫이라고 선언하고 이탈하게 될 것이다.

3. 출발할 때부터 너무 욕심을 내면 안 된다.

천리 길도 한걸음부터라는 속담이 있다. 처음에는 가장 성공 확률이 높은 가장 쉬운 단계부터 시작하는 것이 좋다. 잘못되고 오래된 나쁜 습관을 가진 아이를 단 한번 지도해서 바꿀 수 있다고 생각하는 사람은 없을 것이다. 천천히 자발적으로 이것이 나쁜 습관임을 스스로 자각하고, 올바른 습관을 자발적으로 선택하도록 하는 것이 넛지식 해결 방안이다.

앞으로 소개하게 될 '보안인식(Security Awareness) 강화 프로그램'은 사용자를 쿡쿡 찔러 '자발적'으로 보안에 '참여'하게 하는 것을 목적으로 하고 있다. IT 보안담당자 혼자서만 세우는 보안문화가 아닌, 전체 구성원이 참여하고 협업을 이룰 수 있도록 방법을 제시할 것이다. 제시되는 방법들은 각각의 기업의 문화에 맞게 취사선택돼야 할 것이다. 이러한 방법들은 어떤 기업들에게는 즉각적인 효과가 발생할 수도 있고 효과를 보기 위해 여러 번의 시행착오를 격을 수도 있다.

그동안 보안의 가장 취약한 연결고리로 여겨져 왔던 '사람'에 대한 보안의식 넛지를 통해 보안수준을 제고하고, 경쟁력을 지닌 조직으로 거듭나기를 바란다.