"측정할 수 없으면 관리할 수 없다"

긍정적 착각 활용해 '넛지' … 보안 스토리텔링 필요

연재순서

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

지난 시간에는 넛지의 기본 개념과 사람이 가장 취약한 고리라는 것, 그리고 보안의식 기본 전략에 대해 알아봤다. 이번호에서는 사용자 스스로가 현명한 선택을 하기 위한 구체적이고 실천적인 방법론에 대해 알아보고자 한다.

먼저 품질관리의 세계적 권위자인 에드워드 데밍(Edwards Deming) 교수는 "측정 가능한 모든 것을 측정하라. 그리고 측정이 힘든 모든 것을 측정 가능하게 만들어라"라고 말했다. 또 현대 경영의 구루(guru)로 불리는 피터 드러커(Peter F. Drucker)는 "측정할 수 없다면 관리할 수 없다"라고 언급했다.

이처럼 경영 성과관리에 있어 누구나 공감하고 수긍할 수 있는 공통적 지표는 바로 숫자라고 할 수 있다. 기업의 경우, 경영성과를 측정하거나 신규투자에 대한 사업타당성을 검토할 때 주로 ROI(Return On Investment) 분석방법을 활용한다. 기업의 순이익을 투자액으로 나눈 투자수익률 ROI는 이만큼 투자하면 얼만큼 이익으로 돌아올 수 있는지 측정하는 것으로 모든 비즈니스의 기본이다.

이는 보안에서도 마찬가지인데, 정보보호와 관련한 어떠한 것을 수치로 표현하는 것은 매우 어려운 일이고, 특히나 보안과 관련한 ROI 분석 자체가 매우 힘들다. 그래서 보안관리자들이 경영층을 상대로 "보안 투자는 꼭 해야 합니다. 하지 않으면 심각한 위험에 빠져듭니다"라고 주장하고 설득하는 것은 쉽지 않다.

우리는 이제 에드워드 데밍 교수가 강조했던 것처럼 측정이 힘든 모든 것을 측정 가능하게 만들어야 한다. 조직의 보안의식을 개선하고 보안성을 높이기 위해서는 보안을 측정하여 수치화하는 노력을 포기해서는 안 된다.

그동안 정보보안 분야에서 유일한 글로벌지수는 세계경제포럼이 매년 발표하는 보안서버 보급률이다. SSL 등을 이용해 전송되는 자료를 암복호화해 송수신 하는 서버의 수를 측정하는 이 방식은 특정 벤더의 인증서 수 기준이라는 문제도 있었지만, 보안에 대한 상식이 조금만 있는 사람이라면 이 한 가지 지표로 복잡한 사이버 세계의 보안수준을 평가한다는 것이 얼마나 무모한 것인지 알 수 있다.

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

하지만 일단 평가를 할 수 있다는 것 자체는 중요한 것이다. 또 일부를 가지고도 평가를 가능하게 할 수 있다. 전체에 대한 객관적인 측정이 불가능하다고 포기하고 그대로 방치해서는 개선되지 않는다. 부족하거나 부분적이라 하더라도 우선 측정을 시작하고, 가능한 범위를 늘려 나가는 것이 올바른 방향이다.

보안의식을 평가할 수 있는 도구로, 전사적으로 보안의식을 평가 관리할 수 있는 지니네트웍스의 "지니안(Genian) CAM' 이나 개인정보 영향평가를 할 수 있는 에이쓰리시큐리티의 '알파인더피아(RfinderPIA)' 같은 솔루션을 사용할 수 있다. 하지만 이런 관리도구나 솔루션이 없다고 평가 자체를 할 수 없는 것은 아니다. 취약점분석시스템으로 조직과 개인의 보안의식을 평가할 수 있으며, 기존에 구축해 놓은 보안 시스템들을 얼마든지 활용할 수 있다.

필자는 얼마 전에 모 공사를 방문했다. 그곳은 대규모 조직과 네트워크를 운영하고 있음에도 불구하고 보안에 대한 경영진의 투자가 인색한 편이라 방화벽과 개인용 안티바이러스 제품 등 정말 기본적인 보안 시스템만 운영하고 있었다. 다행히 큰 사고 없이 운영을 해온 보안 관리자가 신기하기도 하고 한편으로는 걱정스러운 마음이 들어 그 동안 어떤 식으로 조직의 보안의식을 평가하고 관리하는지 질문했다.

그곳의 보안 관리자는 백신 제품을 이용해 바이러스에 감염된 PC의 수를 매월 분석하고 수치화해 관련 내용을 회사 게시판에 올리고 있다고 대답했다. 매월 상위 20 개인명단과 감염횟수, 그리고 가장 많이 감염된 상위 5개 부서에 대한 내용을 공개하는 것이다. 게시한 내용이 인사고과에 반영되지 않는 단순 참조용이지만 개인과 부서의 보안의식 부재를 챙기는데 매우 큰 효과가 있다고 한다. 주어진 시스템을 현명하게 활용해 잘 운영하고 있는 예라고 할 수 있다.

필자는 이러한 방법이 매우 좋은 '넛지(nudge)' 라고 생각한다. 부족한 보안의식에 패널티를 주거나 높은 보안의식에 인센티브를 주는 직접적인 방식이 아니다. 대신 사용자의 옆구리를 쿡쿡 찔러 자극을 주는 것이다. 넛지는 전통적인 상벌시스템으로 해결하기 어려운 조직의 문제를 해결하기 위한 수단이다. 따라서 바이러스에 감염된 Top 리스트를 공개하는 것만으로도 보안에 무관심한 사용자들을 충분히 일깨워줄 수 있다.

처음부터 완벽하게 모든 것을 측정하려고 하지 말자. 완벽한 수치화를 추구하려다가 한 발짝도 내딛지 못하고 주저앉게 될 것이다. 우선 측정 가능한 것을 수치화하고, 사용자 피드백을 통해 지속적으로 측정 가능한 것의 범위를 넓혀 나가는 것이 올바른 방향이다. 측정할 수 없으면 관리할 수 없다. 용기를 내자.

효과적으로 사고 사례 전파하기

최근 들어 신문과 방송을 통해 보안사고를 자주 접하게 된다. 금융권, 대기업, 포털 사이트, 해외 글로벌 기업… 심지어는 보안업체에 이르기까지 해킹 대상이 확대되고, 피해 규모는 더욱 커지고 있다. 피해가 심각해지면서 IT 전문지에서만 다뤄지던 내용들이 일간지와 방송을 통해서도 보도됐는데, 이 때문에 일반인들의 해킹에 대한 위험성과 보안의 중요성은 알게 됐다.

지난호에서 인지(Knowing)와 인식(Awareness)의 차이를 언급했는데, 단순히 사고 소식을 자주 접한다고 해서 행동의 변화를 기대하기는 힘들다. 단순히 알아서(Knowing) 할 수 있는 게 아니라 정확한 인식(Awareness)이 있어야 가능하다.

신문이나 방송에서 접하는 보안사고 소식을 내부 사용자들에게 어떻게 효과적인 스토리텔링으로 알려줄 것인가 고민해야 한다. 뉴스를 전하는 언론 내용도 많이 미흡하다. 단순한 위험성을 이야기하는 것은 강 건너 불구경 수준밖에 되지 않는다.

남자들은 군대에서 '사고사례 전파' 라는 내용을 접했을 것이다. 휴가 때의 음주 사고사례나 구타 사고, 군부대 탈영과 같은 내용들이 가장 많은 비중을 차지한다. 군복무 시절 군대 사고사례를 동기들과 함께 재미있게 읽었던 추억이 있다. 군대 내 사고사례는 흥미롭게 읽히는 내용이면서도 그런 사고가 나에게도 일어날 수 있는 일이란 것을 느끼며 경각심을 갖게 해준다.

군의 사고사례 전파 방식과 현재의 보안 사고사례 전파 방식에는 어떤 차이가 있을까? 농협 전산망 마비 사태와 비교해 보도록 하자.

검찰은 지난 4월 발생했던 사상 초유의 농협 전산망 마비 사태를 '북한에 의한 새로운 유형의 사이버 테러' 라고 규정했다. 북한 소행이라는 단어는 우리 내부에 어떠한 메시지도 교훈도 전달할 수 없다. 내부 직원들은 '강 건너 불 구경' 으로 농협 해킹에 대해 이야기할 뿐이다. "설마 내 PC를 북한에서 노려서 침투하겠어?", "그들이 뭣하러 할일없이 내 PC

를 노리겠어?"라는 생각 밖에 들지 않는다.

그렇지만 군에서의 사고사례는 사고 당사자의 인물에서부터 자세히 설명한다. 나이와 평소 성향, 술을 마시면 어떻게 변하는지, 내성적이어서 주변에 동료가 없다든지 하는 인물의 성향과 주변 환경에 대한 설명이 소설처럼 디테일이 살아 있다. 더불어 그 인물 주변의 상황에 대해서도 비교적 상세히 기술한다. 그렇게 인물과 배경에 대해 설명한 후에 사고에 대해 서술한다. 요즘 한창 유행하는 스토리텔링 기법이 살아 있다.

스토리텔링이란 스토리(Story)와 텔링(Telling)의 합성어로 상대방에서 알리고자 하는 바를 재미있고 생생한 이야기로 설득력 있게 전달하는 것을 말한다. 스토리텔링 기법으로 사고사례를 전달하면 보안 사고는 더 이상 나와 상관없는 '강 건너 이야기'가 아니게 된다.

사고가 멀리 있는 것이 아니라 나와 밀접한 곳에 존재하고 있으며, 나나 우리 회사에서 발생할 수 있다는 개연성을 자극하게 된다. 따라서 보안 관리자는 언론과 SNS 등 여러 매체를 통해 전달되는 보안사고 소식과 자료를 스토리텔링 기법으로 전달해야 할 것이다.

최근 발생한 RSA에서 보안 사고를 스토리텔링으로 내부 사용자에게 전달하는 것을 예로 들어 보겠다.

효과적인 사고사례 전파의 초점은 무엇보다도 외부에서 발생한 보안 사고가 '강 건너 불구경'이 아니라 조금만 방심하면 나와 내 주변에서도 쉽게 일어날 수 있는 사고임을 전달하는데 있다.

또한 사고가 발생했을 때의 즉시성 있는 스토링텔링 사고사례 전파는 일반 보안교육보다 사용자들의 보안의식을 확실히 일깨워 줄 수 있으며, 시간과 비용도 줄일 수 있어 일석이조의 효과를 낼 수 있다.(상자 참조)

RSA 해킹 사고로 인한 정보 유출

지난 4월 1일 유명한 보안업체인 RSA에서 중요 기술정보가 해킹으로 유출되는 사고가 있었다고 합니다. 참 아이러니한 일이 아닐 수 없습니다. RSA는 보안성이 매우 높은 보안제품을 개발하는 회사며, 미국 기업과 은행뿐 아니라 군부대에서도 많이 사용되는 기술을 제공하는 곳인데도 불구하고 해커의 공격으로 정보가 유출된 것입니다.

사건은 이렇습니다. 공격자는 페이스북, 트위터 등에서 RSA 직원의 정보를 수집하고 이들에 걸쳐서 두 개의 그룹에게 피싱 메일을 보냈다고 합니다. 해커는 '2011 채용 계획'이란 제목으로 사람들을 유혹했습니다. 요즘 선정적인 제목이나 업무와 관련된 듯한 제목으로 악성코드를 첨부한 메일을 보내 공격을 시작한다고 합니다.

다행스럽게도 공격자의 메일은 스팸 메일로 처리돼 〔정크메일함〕으로 들어갔는데, 호기심 많고 부주의한 직원 하나가 정크메일 박스에서 '채용 계획'이란 제목의 이메일을 발견하고 열어 보았다고 합니다. 엑셀로 된 첨부파일에는 어도비 취약점을 이용한 공격코드가 심어져 있었습니다. 이에 해당 직원의 PC는 좀비PC가 돼 외부에서 조정할 수 있게 됐고, 이를 통해 내부 정보가 유출됐다고 합니다. 현재는 해당 공격 관련 패치가 나와 있는 상태입니다.

보안회사로 이름을 떨치던 회사가 한 직원의 실수로 인해 브랜드 이미지에 치명적인 손실을 입고 말았습니다.

교훈

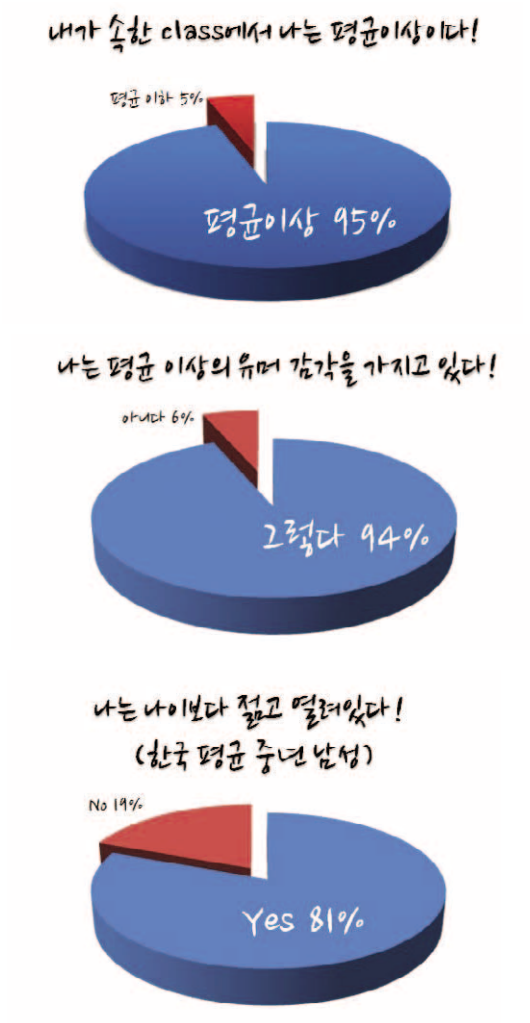
1. SNS 등을 사용할 때는 회사 이메일 등 개인정보 공개에 주의해야 합니다. 만약 공개돼 있다면 해당 정보를 즉시 삭제해야 합니다.
2. 시스템에 의해 스팸메일로 분류된 정보는 각별히 유의해야 합니다. 함부로 열어 보면 절대 안 됩니다.
3. 우리회사는 '채용 계획' 등을 개인 이메일로 보내지 않습니다. 기존에 없었던 형식으로 메일이 온 경우, 해당 팀에 전화해 확인해야 합니다.
4. 플래쉬를 지원하는 어도비 관련 공격이 많이 나오고 있습니다. OS 패치하듯이 어도비 업데이트 실행창이 뜨면 반드시 업데이트 해야 합니다.
5. 한 개인의 실수가 회사에 치명적인 피해를 끼칠 수 있습니다. 각별히 주의해야 합니다.

긍정적인 착각의 활용

사람들은 그룹에 속해 있을 때 '나는 항상 평균 이상이다'라는 긍정적인 착각을 하기 마련이다. 사람이 자기 자신을 평가할 때는 '해석'이라는 요소가 수반되며, 가급적 낙관적인 해석을 가미하는 경향이 있기 때문이다. 연구 결과나 설문 조사 결과들을 살펴보면 우리가 생각하는 것 이상으로 긍정적인 착각이 많이 작용하는 것을 알 수 있다.

미국의 한 학급에서 학생들을 대상으로 '이 학급의 성적 분포를 십분위로 나누었을 때 당신은 어느 범주에 들것으로 예상하는가?'라는 무기명 설문조사를 실시했다. 어떤 학급이든 절반이 상위 50%에 들면 나머지는 하위 50%에 들 수밖에 없다. 그런데 조사 결과 대개 자신이 중간 이하일 거라고 기대하는 학생은 5% 미만에 불과했으며 상위 20%에 들 것이라고 생각하는 학생은 절반 이상에 달했다. 즉 학생들 대다수인 95%가 자신이 이 학급에서 평균 이상이라고 생각

〈그림 1〉 주변에서 쉽게 볼 수 있는 긍정적인 착각



한다는 것이다.

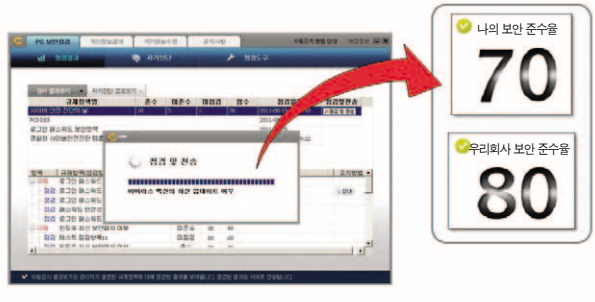
학점이라는 명확한 평가와 기준이 있음에도 불구하고 어떻게 이런 착각이 가능할까? 학점을 C, D로 도배했을지라도 "내가 당구치고 노느라고 그랬지… 이 정도 놀고 이 점수 나왔다면 나는 평균이상이야!"라는 대단한 착각을 하고 있다는 것이다.

국내에서도 비슷한 설문결과가 있다. 40대 이상 중년 남성을 대상으로 '나는 동년배에 비해 젊고 오픈 마인드다!'라는 설문에 약 80%가 '그렇다'라고 대답했다. 이상하다, 우리 주변에 있는 속 좁고 고리타분한 그 많던 아저씨들은 다 어디로 사라진 것일까?

유사한 설문 결과 사례들이 많다. '나는 평균 이상의 운전 실력을 가지고 있다?', '나는 평균 이상의 유머 감각을 가지고 있다' 등 각종 설문 조사에서 80~90%의 사람들이 '그렇다'라고 대답한다. '평균 이상'의 효과는 우리가 찾고자 하면 어디서나 찾아볼 수 있다.

넛지(nudge)는 이러한 긍정적 착각을 보안의식 개선에 활용하는 것이다. 우리 회사에서 개발하고 현재 내부에서도 하고 있는 '지니안 CAM'은 개인의 PC에 대한 보안 수준을 진단하고 평가해서 조치 방법들을 알려준다. 각자에게 본인의 점수와 회사의 평균 점수를 비교해 보여주는데, 회사 평균점보다 점수가 더 낮은 직원이라면 '엇! 내가 적어도 우리 회사에서 평균 이상은 되지!'라는 생각을 하고 미흡한 보안부분을 개선하게 되는 것이다.

〈그림 2〉 지니안 CAM에서 보여주는 개인과 회사의 보안준수율 비교



사용자에게 문제점과 조치 방법을 알려줬지만 꿈쩍도 하지 않았다. 코끼리는 별로 신경 쓰지 않는 것이다. 그냥 매번 PC보안 평가 결과를 모았을 뿐이었지 확연한 개선의 여지가 보이질 않았다. 그러나 이런 넛지식 방법을 이용하니까 움직이지 않던 코끼리가 꿈틀대고 반응하기 시작했다.

적어도 평균 이하인 '열위'라는 평가는 누구도 받지 않으려고 한다. 긍정적인 착각을 효과적으로 사용하기 위해서는 어떤 기준이든 간에 측정하고 수치화할 수 있는 데이터를 제시하는 것이 효과적이다. 측정하고 수치화할 수 있는 데이터가 있다면, 사용자에게 제시해 "당신이 우리 회사에서 평균 이하에 속하고 있다"라는 메시지를 던지는 것만으로도 사용자 스스로 보안환경을 개선할 수 있도록 깨울 수 있을 것이다.