情 報 保 護 學 會 誌
第 16 卷 第 2 號, 2006. 4

효과적인 정보보호인식제고 방안

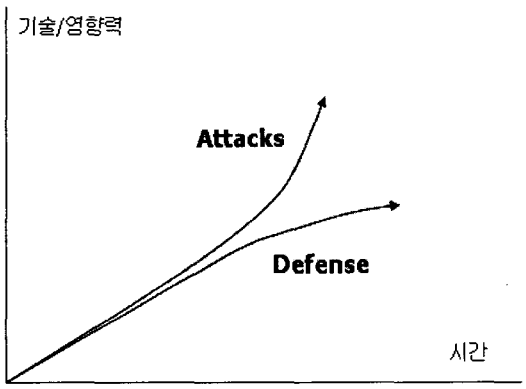
임 채 호*

요 약

최근 정보보호분야는 공격기술이 방어기술보다 더 뛰어난 상태이며, 이는 사회공학, 악성코드, 제로데이 공격 등으로 인하여 정보보호 솔루션을 아무리 이용하여도 막을 수 없는 것이다. 그러므로 정보보호를 모든 참여자들이 생활화하기 위한 정보보보인식제고 프로그램 효율적으로 진행하기 위한 방안을 기술한다.

Ⅰ. 현재 정보보호 문제점

오늘날 정보보호는 공격기술이 정보보호기술보다 더욱 앞선 상태를 오랫동안 지속하고 있는 상황이다. 인터넷의 급격한 발전에 따르는 사회의 변화는 인터넷 보안 문제 및 위협상황을 보다 복잡하게 발전시켜 이를 막아야 하는 정보보호는 기술적인 진전만으로는 해결하기 어려운 상황이 된 것이다.



〔그림 1〕 공격과 방어의 차이

공격이 방어보다 앞서가는 현실은

- 악성코드 공격(Malicious Attacks)
- 제로데이 공격 및 DoS/DoI 공격
- 사회공학 및 금융, 개인정보보호 공격

등에 기인하고 있는 바가 크다. 다음 그림은 공격의 양상을 보여주고 있다.최근 이슈가 되고 있는 P2P, Phishing, 개인정보 유출, 스파이웨어, 스팸 등 다양한 공격기술은 사회공학적 공격기법과 합류되어 기술 및 솔루션이 막을 수 없는 상황이 진행되고 있다. 정보보호 인식제고를 하지 않으면 안될 일들이 벌어지고 있는 것이다.

사실 정보보호 인식제고는 정보보호를 추진하는 모든 조직과 주체가 당연히 기본적으로 하여야 할 ISMS(Information Security Management Structure) 상에 있어야만 하는 매우 중요한 요소 중의 하나인데도 불구하고 아직도 체계적인 수행방안이 안되고 있는 것이 사실이다.

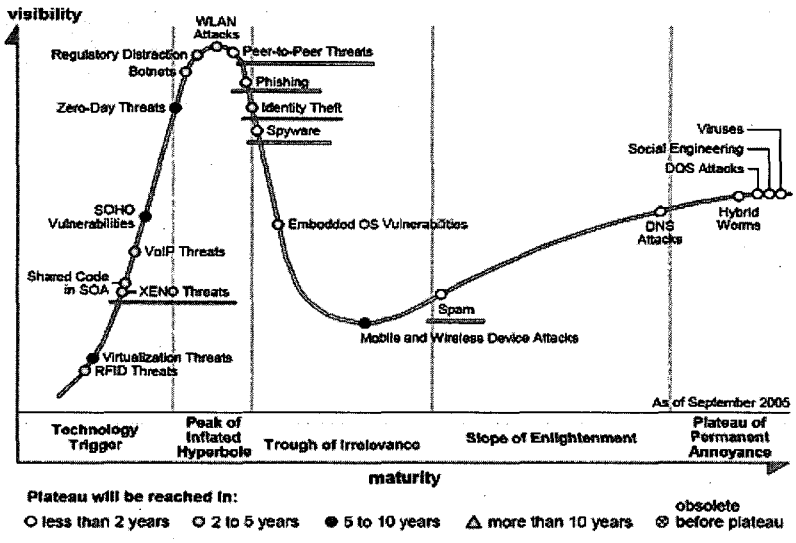
이번 논문에서 정보보호 인식제고를 실무적 차원에서 정의하고 필요성을 제기한 후 국내에서 어떻게 추진하면 좋을 지 피력하고자 한다.

Ⅱ. 정보보호 인식제고에 대한 개념

2.1 개요

만약 자신에게 수신된 전자우편 중 고위공무원 부정축재자 명단이 첨부하였다는 메일을 받는다면 첨부를 열어볼 것인가? 만약 유명 금융기관이 자신의 인터넷 뱅킹 이용환경이 금융기관의 시스템 변경으로 구좌번호, 비밀번호를 입력하라면 어찌하겠는가? 만약 인터넷 포탈을 검색 중 재테크에 관심을 가진 사람이 솔깃한 정보가 있다면 클릭할 것인가? 만약 노

* 박사/nhn 보안담당수석 skscogh@nhncorp.com



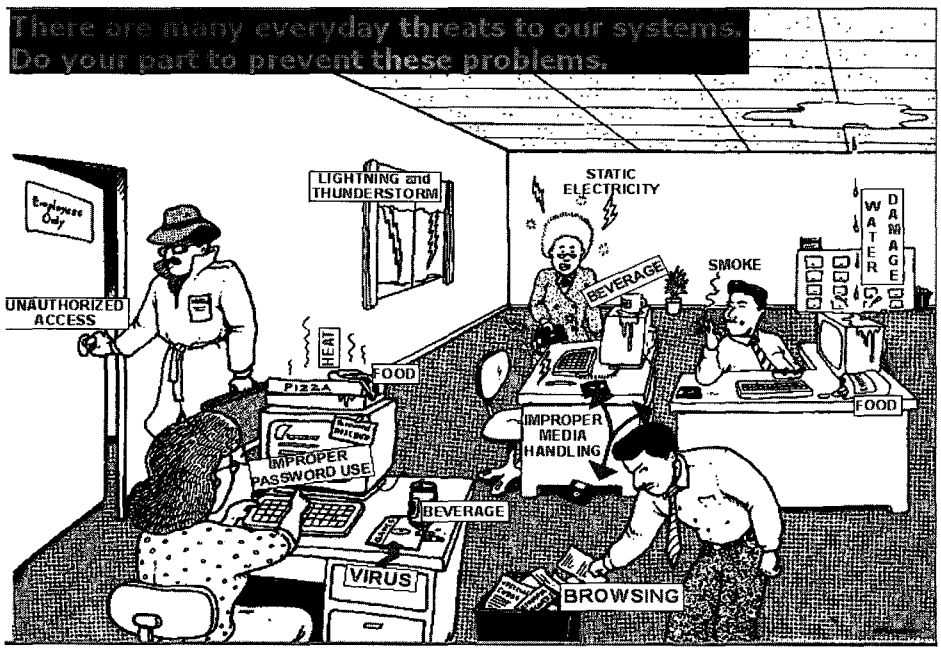
〔그림 2〕 사이버위협의 전개

트북이 필요한 상황에서 반값에 판매하는 사이트 정보가 있으면 이를 믿고 계좌에 돈을 입력할 것인가?

이 모든 사례가 인터넷을 이용하는 모든 사람이 자칫 잘못하면 걸리는 사기이다.

이밖에도 한 조직에 근무하는 직원이 조직의 보안을 위하여 지켜야만 하는 많은 사항들이 있다. 물론 정보보안을 담당하는 직원이 만든 정보보호 기술 및 솔루션이 하지 못하는 많은 사항들이 직원 개개인이 지켜야만 할 사항들인 것이다.

다음 그림은 어떤 사무실 환경을 보여주고 있다. 직원들이 각자 지켜야만 하는 많은 정보보호 수칙들을 모든 직원들이 잘 지켜가는 상황인지 확인하여야 할 것이다.



〔그림 3〕 정보보호 인식제고와 사무실 환경

2.2 정보보호 인식제고의 정의

정보보호인식제고(Security Awareness) 의 정의는 다음과 같다.

- 사람들이 자신의 직무를 수행하는데 있어, 정보보안의 함축된 상태를 잘 알 수 있도록 하는 프로세스
- 여기에는 정보보호의 중요성인식, 보안사고 발생시 이에 대한 대응방안과 보고체제 등이 포함된다.
- 결국 "정보자산의 위협관리에 대한 지행합일(知行合一)의 상태를 의미
- 잠재적인 위협을 이해하여 조직 구성원이 매일 매일 일상적 업무에서 겪을 어떤 보안이슈와 사고를 알게 되는 장점
- 정보보안 기술은 정보보호에 혼자서 생존할 수 없으며, 조직 구성인과 개인정보보호 책임 및 인식제고 정보보호 프로그램 성공에 가장 중요

정보보호인식제고는 조직의 정보자산에 대한 조직 구성원의 정보보호를 보안정책에 따라 적절한 정보보호 인식제고를 수행하여야 한다. 결국 정보보호인식제고는 자산, 정책, 정책 및 정보보안인식교육이 자리잡는 것이다.

2.3 정보보호인식제고 구현 모델

정보보호인식제고는 다음 〔그림 4〕 정보보호관리 모델에서 볼 때 조직의 정보보호를 이끌어가는 가장 큰 축의 하나이다.

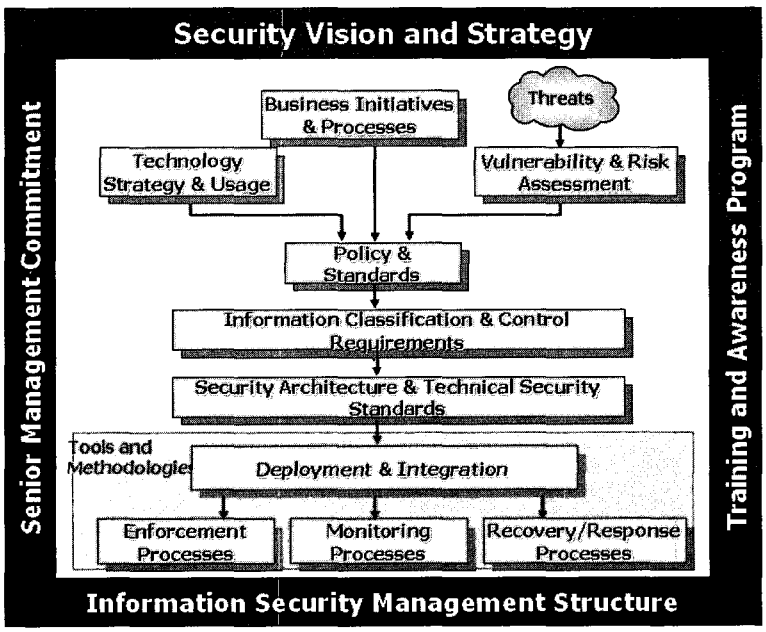
정보보안인식제고가 성공적이라면, 조직이 갖게 되는 사항은 다음과 같다.

- 조직의 보안 기능을 적절하게 사용할 수 있도록 해준다.
- 직원들이 이상한 보안문제, 잠재적으로 악의가 있을 사항을 보고하게 한다.
- 보안의 심각성을 깨닫게 하므로 직원들의 근면함을 일깨운다.
- 조직의 위험관리 상 가장 중요한 것임을 깨닫게 한다.

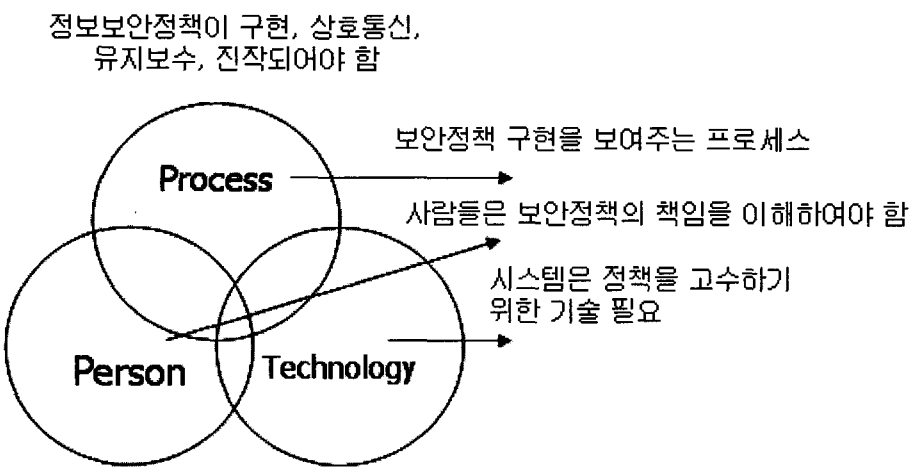
2.4 정보보안인식제고 원칙 및 구현사항

정보보안인식제고의 4가지 원칙인 4R은 다음과 같다.

- Relevance(적절성원칙) : 개별 직원 별로 인식제고가 전달되어야 함
- Role(역할부여) : 소유자, 고객, 이용자 별 임무 부여



〔그림 4〕 정보보안관리체계와 정보보안인식제고



〔그림 5〕 정보보안인식제고 프로그램구현

- Responsibility(책임부여) : 각자 자신의 본분에 맞게 인식제고
- Repercussion(반향성) : 정책에 알맞게 각자 적용되어야 함

이러한 4R에 따라 인식제고의 원칙은 다음과 같이 볼 수 있다.

- 주목하게, Attention Getting
- 적절한 담당자, Appeal to target audience
- 기본학습으로 단순하고,기억하게, Basic-keep it simple and memorable
- 강압적이지 않게, Buy-in is better than coercion
- 최신의, Current
- 신뢰할 수 있는, Credible
- 지속적인, continuing

이러한 원칙에 맞게 인식제고 프로그램을 기획한다면, 성공적인 프로그램을 만들기 위하여, 다음이 요구된다.

- 요구사항을 잘 분석하여 충족하여야 하며,
- 공식적인 산출물 도출을 위한 계획안을 만들고,
- 구현되었을 경우의 가치를 가시적으로 보이고,
- 이러한 프로그램을 모든 이에게 전파되어야 한다.

그래서 성공적인 프로그램은 다음을 만족하여야 한다.

- 지속적으로 수행되어 "나는 몰랐어" 라는 표현이 나오지 않게 하여야 함
- 잘 이해되게 제작되어 모든 직원이 인식되어야 함
- 잘 전달되도록 다양한 매체나 미디어를 활용함
- 측정 가능하도록 저비용의 효과적인 추진을 가능하여야 함
  - 직원 통과, 사회공학공격, 직원 Survey 취합, 패스워드 크래킹 도구 사용 등

2.5 인식제고 프로그램 설계

인식제고 프로그램은 전달방법(Delivery Method), 전달내용(Topics/Contents), 시의적절성(Timeliness), 효과성(Effectiveness) 가 필요하다.

전달 방법은 다음과 같은 종류가 있다

• 뉴스레터,	• 인트라넷,	• 전자우편,
• 보이스메일,	• 브리핑,	• 세미나,
• 비데오,	• 교육훈련,	• 전문백서,
• 논문,	• 이벤트 공시,	• 사고노트,
• 포스터,	• 콘테스트,	• 매뉴얼,
• 노트,	• 설문조사,	• 인식제고의 날,
• 화면보호기,	• 인식제고프로그램,	• 검사,
• 감사,	• Audit,	• 방송

또한 인식제고 내용은 다음과 같은 것이 있다.

- 사무실 책상 정리정돈
- 시스템(PC) 정지 절차

- 비밀정보 안전 저장 방법
- 재활용 및 파기 방법
- 패스워드 만들기 및 관리
- 바이러스 탐지 및 대응
- 백업 및 데이터 저장관리
- 장치의 시설물 통과 절차
- 노트북 보안
- 암호기능 사용법
- 전자우편 이용법
- 데이터 분류 및 사용법
- 사내망 이용법
- 원격 접속방법
- 공중 전화 및 핸드폰 이용
- 사회공학 회피
- 일반 법령 및 시행령

물론 경영자나 관리자, 일반 직원 등 각 분야별로 별도의 인식제고 프로그램을 제작하고 운영할 필요가 있다. 이는 광범위한 인식제고, 특정층 인식제고, 개개인 인식제고 등이 구현 상의 옵션이 될 것이다.

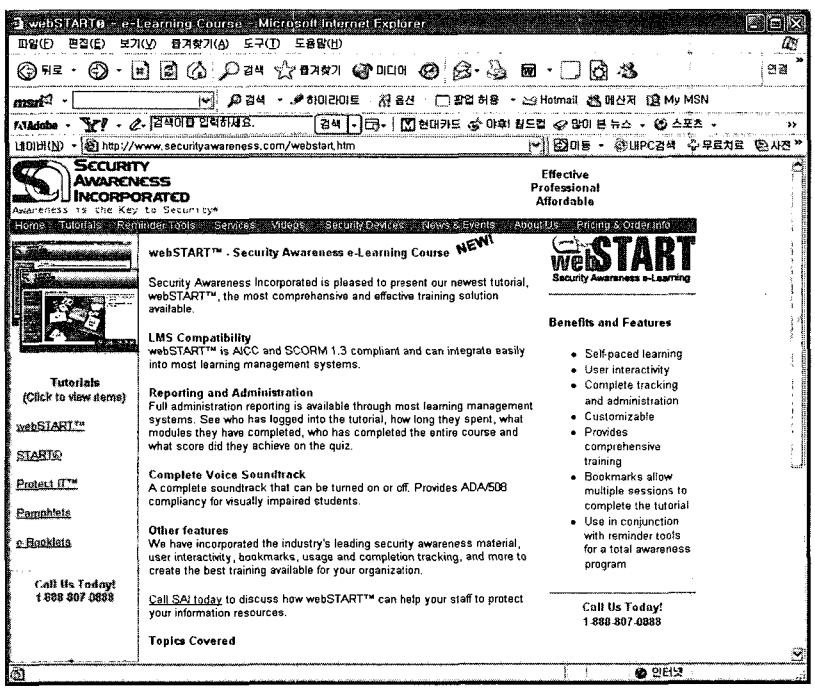
인식제고 프로그램을 제공하는 사이트는 www.securityawareness.com 을 참조로 보면 적당하다. 특히 여기에는Self Learning System 인 START(Security Training and Awareness, Reference Tool) 를 제공하고 있으며, WebSTART도 제공한다.

Ⅲ. 정보보안 자기교육시스템(Self Learning System)

3.1. 개 요

정보보안은 어떤 조직에서도 강하고 잘 견디는 확고한(Robust) 체계 마련이 가장 절실하게 된다. 이는 안전하고(Secure), 효율적이고(Efficient), 검증된(Assurance) 보안관리 체계가 요구된다. SEA 환경은 비밀보장(Confidentiality), 무결보장(Integrity), 가용보장(Availability) 등의 정보보호 목표인 CIA 를 구현관리하기 위한 바람직한 이행요건이 될 것이다.

정보보안의 성공 요건은 모든 직원의 정보보호 참여만이 가장 필요하고 모든 직원의 정보보안 인식을 개선하여 행동하는 정보보안 생활화는 인식제고 프로그램의 성공 여부에 달려있다. 정보보안에 대한 프로그램을 운영하면서 다른 전문가의 가르침 보다 스스로 익히게 하는 것이 더욱 효과적임을 누구나 알 수 있다.



〔그림 6〕 Securityawareness 의 WebSTAST

- 자기주도를 통한 인식을 제고하여, 확인 능력과 책임감 부여 가능
- 프로파일 비교 분석을 통한 객관성 확보
- 학습 경로선택의 다양화를 통한 주관성 가능
- 재 학습을 통한 수정 피드백 가능
- 학습 종료 후 커뮤니티 연계 가능

3.1.2 WebSTART

WebSTART는 다음과 같은 특징이 있다.

- 자기 주도형 학습
- 사용자 대화 가능
- 완벽한 과정 추적 및 관리 가능
- 고객 요구에 맞게 수정 가능
- 완벽한 이해를 돕는 교육훈련
- 복수개의 세션 교육훈련 가능
- 전반적인 교육 훈련에 효과적인 참여 가능

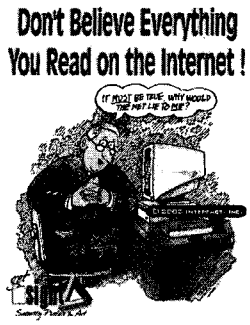
지금 현재의 교육내용은.

- 패스워드 제작 및 관리
- 인터넷 안전 이용
- 전화 이용 및 사기 방지
- 물리적 보안
- 전자우편 안전 사용
- 개인정보 보호
- 컴퓨터 바이러스
- 개인 컴퓨터 보안
- 소프트웨어 라이센스
- 백업 구축
- 접근 통제
- 사회공학
- 개인신원 도용 방지

등이다.

3.1.3 개인별 학습 내용

Ⅳ. 결 론



현재 공격기술이 방어기술 보다 매우 앞선 상황에서 전 조직원이 참여하는 보안생활화가 요구되는 정보보안인식제고는 정보보안의 가장 중요한 구성요소가 될 것이다. 이 논문을 통하여 정보보안 인식제고가 무엇이며, 그 구현방법, WebSTASRT를 통한 자기학습방법 등을 살펴보았다. 새로운 공격기법 및 사회공학 공격 등에 가장 올바른 대응 방법은 인식제고임을 알아야 할 것이다.

참 고 문 헌

[1] SANS Papers: "Security Awareness: Preventing a Lack in Security Conscious ness", Katherine Ludwig, May 25, 2001. http://rr.sans.org/aware/lack.php

[2] "Introduction and Education of Information Security Policies to Employees in My Organization", Harbinder Kaur, August 29, 2001. http://rr.sans.org/aware/infosec_policies.php

[3] Microsoft offers two free security aware ness screen savers: the Ten Immutable Laws of Security, and one that dis plays the Ten Immutable Laws of Security Administration. http://www. microsoft.com/Downloads/Release.asp?Rel easeID=26684

[4] Cybercitizen Awareness Program probably not too useful for professional organizations, but I include it because it illustrates that security awareness can begin at any age.

구 분	내 용	비 고
역량 진단	카테고리 역량 진단	결과 제공
프로파일링	학습 타입 결정	우선 순위 제공
컨텐츠	학습규칙, 자료 제공	개인별 차별화
커뮤니티	핵심역량, 커뮤니티 관리	운영 가능
맵/로그인	컨텐츠맵, 프로파일 생성 등	

http://www.cybercitizenship.org/
[5] Computer Security Institute. This company offers security awareness newsletters, security alerts, and security assessment kits, among other things. https://wow.mfi.com/csi/order/publications.html
[6] Interpact, Inc. offers a variety of services including awareness programs, seminars, brochures, artwork, and others. http://www.interpactinc.com/home.htmlNative Intelligence, Inc. They offer a variety of awareness services including tutorials,
[7] posters, screen savers, animations, and haikus to help educate your personnel. http://www.nativeintelligence.com/
[8] Security Awareness Inc. This company has several offerings including tutorials, posters, screen savers, an awareness workshop, banners, and other educational tools. http://www.securityawareness.com/
[9] Security Web Sites offers a customizable website service, and awareness presentations. http://www.securitywebsites.com/
[10] 임채호, SIS03, "효과적인 정보보호 인식제고 방안", 2003. 7

〈著 者 紹 介〉

임 채 호 (Lim Chae-Ho)
종신회원

1979-1986 홍익대학교 전산학과 학사
1987-1990 건국대학교 전산학과 석사
1992-2001 홍익대학교 전산학과 박사
1985-1991 KIST/시스템공학연구소 선임연구원
1992-1995 대전 우송정보대학 교수
1996-2000 한국정보보호진흥원 책임연구원
2001-2003 한국과학기술원 전산학과 초빙교수
2003-2005 시큐리티맵(주) 대표이사
2006-현재 nhn 보안 수석