제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

중등학교의 보안성 평가를 위한 지표 개발에 관한 연구

고 진 홍* 안 성 진*
* 성균관대학교 교육대학원 컴퓨터교육전공

요 약

학내 전산망은 정보의 주도로 교수학습에 필요한 네트워크 자산을 통한 교육적인 활동을 지원하기 위해서 많은 학교에 설치되었다. 반면에 인터넷의 개방성과 학내 전산망의 보안 실태 때문에 내부자나 정보를 얻고자하는 하는 해커들에 의하여 상당한 피해를 당하고 있다. 그러므로, 본 연구에서는 학내 정보자산을 분류하고 보안항목 및 문제점을 제시하고 있다. 마지막으로, 정보자산의 부분별로 효율적이고 조직적으로 평가 지표를 제시하였다.

A Study on the development of metrics for security evaluation of secondary schools

Jin hong Ko* Sung Jin An*

ABSTRACT

School Networks environment is implemented in many schools to support educational activities for networking resources required in teaching-learning activities with government initiative. On the other hand, the open system in school which are used in internet in internet do considerable damage committed by intruder and cracker to the preservation of computer data and system due to second schools security state. Therefore this study is to present assortment in information resources of schools, security items and problem. finally, we give the effective and systematic metrics of estimates for security of secondary schools in information resources parts.

1. 서 론

우리 사회는 네트워크가 사회적, 문화적 기반이 되는 본격적인 지식정보화사회로 접어들고 있다. 교육도 이에 부합하듯 현재 전국의 모든 초·중·고등학교의 21만여 개의 교실에 초고속 인터넷이 연결된 교육인프라가 구축되었다.[1] 이에 교육인프라를 통한 정보와 지식의 창출, 정보의 유통 및 활용이 활발하게 하는 등의 순기능으로 국가경쟁력 향상을 도모하고 있다.

반면에 인터넷을 통한 학내 전산망 불법적인 침입으로 내부 시스템 정보가 유출되거나 파괴되는 현상이 발생하고 있다. 특히, 인터넷의 개방적인 특성 때문에 온라인 성적 처리 혹은 보관된 성적의 데이터가 수정, 침해 등의 사건이 발생될 수가 있고 선생님들의 시험출제 문제 및 수행평가 성적 등 각종 학사관련 자료와 중요한 문서들, 학교운영에 관련된 자료들에 대해서도 외부의 침입 가능성이 항상 존재하고 있다. 또한 내부 사용자에 의한 정보의 유출 현상들도 발생할 수 있다. 따라서, 외부의 침입과 내부 사용자들의 자료 수정 및 위조 등으로부터 보호하기 위하여 일반중등학교에서는 학교 전산망에 대한 보안을 위한 노력을 기울이고 있다. 하지만, 보안에 대한 지표나 기준이 미약한 것은 사실이다. 이번 연구를 통한 보안 지표를 마련하고자 한다.

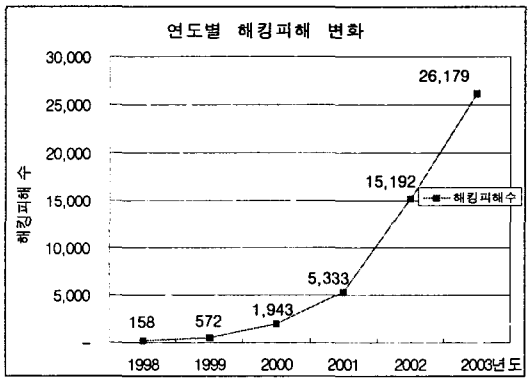
2. 중등학교 정보 보안

2.1 중등학교 정보보안의 중요성

최근의 학교 현장에서 이용하고 있는 교육행정정보시스템(National Education Information System, 이하 NEIS이라 지칭한다)이란 전국의 1만 여 개의 초·중등학교와 시·도 교육청, 산하 기관, 교육인적자원부를 인터넷으로 연결하여 교육관련 정보를 공동으로 이용할 수 있도록 전산환경을 구축하는 시스템이다.[2] NEIS는 인터넷 프로토콜의 취약성 때문에 학생 신상 정보, 학부모 정보, 성적관련 정보, 혹은 관련된 개인적인 정보 등과 로그인 비밀번호 등의 중요한 정보들이 쉽게 노출될 수 있다.[3] 따라서, 수요자 측면의 개인정보 보호의 중요성이 강조되고 있는 시점에서 NEIS 전반에 걸쳐 적절한 정보보호 장치가 없다면 시스템 자체가 존재하기 어렵게 될 것이다. 또한, NEIS는 학내 전산망 토대 위에서 이루어지기 때문에 학내 전산 시스템의 보안의 중요성이 날로 높아지고 있다.

2.2 학교 전산망의 해킹 동향

교내에서 사용하는 교직원들의 PC는 대부분 윈도우 계열로 구성되어 있으며, 보안의식의 부족으로 인하여 해킹의 위험에 노출되어 있다.



(그림 1) 연도별 해킹피해 변화

최근 한국정보보호진흥원이 발표한 2003년 해킹 바이러스 동향'에 따르면 2003년에는 총 2만 6179건의 해킹 피해가 국내에서 발생했다. 이는 지난 98년의 158건과 비교하면 5년 만에 무려 165.7배나 증가한 수치다.

최근 국가정보원이 발표한 '국가기관 침해사고 대응현황'에 따르면 2002년 1월1일부터 6월7일까지 발생한 해킹사고의 가장 큰 특징 중의 하나는 보안관리기관과 그렇지 않은 기관 간에 사고 발생 비율이 현저히 차이가 난다는 점이다. 보안 담당자 및 각종 보안 시스템이 설치되어 있는

등 상대적으로 보안관리가 철저한 중앙행정기관은 발생건수가 적었던데 비하여 예산 및 인력부족으로 적절한 보안조치를 강구하지 못한 초중고 등 교육기관은 총 475건이 발생해 전체 기관별 해킹 사고 발생 건수의 81.8%를 차지했다. 이는 2001년 전체 507건 중 331건으로 65%를 차지했던 것에 비해 급격한 증가세를 보이고 있다. 이는 공공기관 가운데 교육기관이 해킹에 가장 취약하다는 증거이다. 특히, 대부분의 교육기관은 해외 해커가 다른 나라의 기업이나 공공기관을 해킹하기 위해 경유지로 이용하는 것으로 알려졌다.[4]

2.3 학내 전산망의 보안 실태 및 문제점

인터넷이 대중화되면서 초·중등학교에 전산망이 구축되고 전용선 등을 통한 인터넷 망(WAN)과의 연결이 일반화되었다. 학내 전산망이란 단위학교에 설치되는 각종 정보기기를 상호 연결하여, 데이터를 교환하거나 공유할 수 있도록 하는 통신장치로서, 내부의 근거리 통신망(LAN)구성 장치와 외부망과 접속하는 장치들을 모두 말한다.[5] 학내 전산망을 통하여 교수학습 및 학생에 관련된 정보가 상호 이동되며 학교생활 전반에 걸쳐서 편리하고 효율적인 정보 활용 및 가공을 할 수 있게 되었다.

현재 학내 전산망(학내망이라고도 한다)의 보안 실태 및 문제점을 다음과 같이 제시한다.

첫째, 학내 보안관리의 중요성 인식 부재를 들 수 있다. 초·중·고교 해킹사고가 증가하는 것은 학내망의 인터넷 연동구축사업으로 이루어진 정보화사업이 시스템 구축에만 신경을 쓰고 보안 관리 대책에 소홀했기 때문이다.

둘째, 학내망을 전담하는 관리자의 부재이다. 일반적인 단위학교의 경우 학내시스템의 관리자가 현직 교사로서 시스템 관리 이외의 교직업무를 동시에 수행해야 할뿐만 아니라 시스템 자체에 관한 이해 및 지식이 부족하여 시스템 관리에 허점이 많음을 나타난다.[6]

세째, 학내망을 위탁 운영하고 있는 유지보수 업체의 보안관리 소홀을 들 수 있다. 대개 중소규모의 학내 보수유지 업체의 난립으로 실력이 검증되고 서비스 의식이 투철한 업체의 전산망 피해 문제 해결을 보기가 힘들다.

넷째, 학내망 사용자들의 ID 패스워드 관리 태만을 들 수 있다. 교사들이나 교직원 및 학생들은 개인정보 보호의식이 일반 기업들에 비하여 뒤떨어진다. 일례로, NEIS의 업무처리 시에 다른 교사 ID로 작업을 처리하는 경우도 있다.

다섯째, 보안에 대한 투자와 교육이 미흡하다. 해킹사고를 막기 위해서는 방화벽이나 침입탐지시스템(IDS)등 각종 정보보안 시스템을 구축하거나 지속적인 업그레이드를 해야 하지만 학교재정상 어려운 실정이고, 보안에 대한 전문적이고 수준 높은 교육을 받는 경우가 적었다.

3. 정보자산의 보안 평가 및 지표

3.1 보안의 기본목표

정보보안은 내부·외부의 침입자에 의한 파괴, 변조 및 유출 등과 같은 정보 범죄로부터 내부의 정보를 보호하는 것으로 최근의 해킹과 바이러스에 의한 교육정보의 유출, 파괴, 변형 등의 위험성이 커지는 시점에서 그 중요성이 부각되고 있다. 정보 보안의 기본 목표는 다음과 같다.

첫째, 기밀성(Confidentiality)을 유지하여야 한다. 기밀성이란 인가를 받은 사람만이 접근할 수 있어야 하며, 인가되지 않은 정보의 공개는 금지되어야 한다는 보안 요구사항이다. 기밀성을 유지하기 위해서는 접근통제 메커니즘과 암호화 기법 등이 있다.

둘째, 무결성(Authentication)을 유지하여야 한다. 무결성이란 비인가자에 의한 정보의 생성, 변경, 삭제를 보호하여 정확성이 보장되어야 한다는 보안 요구사항을 말한다. 무결성을 통제하기 위해서는 물리적 수준에서의 접근통제와 운

영체제 · 네트워크 수준에서의 접근통제가 있다.

세째, 가용성(Availability)을 유지하여야 한다. 가용성이란 정당한 권한이 주어진 사용자에게 정보서비스를 거부하여서는 안 된다는 보안 요구사항이다. 가용성을 확보하기 위한 통제수단에는 데이터의 백업, 시스템의 이중화, 물리적 위험으로부터의 보호 등이 있다.

네째, 인증성(Authenticity)을 유지하여야 한다. 학내 정보자산을 사용할 때 사용자들을 확인해야한다. 인증성에는 반드시 사용자만이 인증 대상이 되는 것이 아니고 컴퓨터 시스템 및 응용 프로그램 등도 포함될 수 있다. 외부에서 내부의 정보자산에 침입하는 경우를 대비하여 정확하게 인증대상을 확인하는 기능이 제공되어야 한다. 데이터 송신은 암호화된 데이터 영역과 송신측 주소를 보내면 수신측 에서는 복호화한 후 주소를 확인함으로써 실현될 수 있다.[7]

3.2 정보 자산의 분류

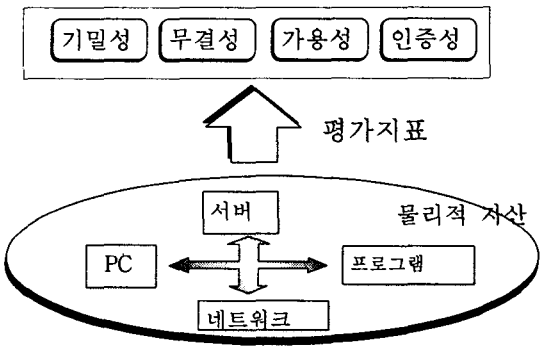
학교 내의 정보 자산을 분류하기가 쉬운 일이 아니다. 서버나 개인 PC에 보관돼 있는 정보에는 구체적으로 어떤 내용들이 들어있는지 조차도 알지 못하고 있는 현실에서 정보보안의 기초를 더욱 어렵게 만들고 있다. 다음은 학교 내에 있는 유형별 자산을 소개한다.

< 표 1 > 학내 정보자산의 분류

유형별	내 용	소분류
네트워크	네트워크서비스/학교업무와 관련된 장비 및 소프트웨어	라우터, 스위치,허브, 케이블
보안시스템	침입차단 시스템과 침입탐지시스템과 같은 정보자산보호를 위한 각종하드웨어 및 소프트웨어, 서버시스템 및 네트워크에 같이 포함됨	방화벽, IDS
서버시스템	교내외 서비스/업무 및 업무, 홈페이지를 위해 사용되는 서버로 운영체제 및 유틸리티 등 시스템 소프트웨어 포함	방화벽서버 프락시서버 웹 서버 파일 서버
프로그램	소프트카피나 하드카피로 보관중인 각종 소프트웨어	교수학습프로그램, 업무관련프로그램
전자정보	데이터베이스, 데이터파일 등 전자적 형태로 저장하는 정보, 교수학습에 관련된 정보나 학교업무 처리에 관련된 정보	NEIS정보 학습교안 학생자료
PC	교사나 학생들이 교수학습 및 업무용으로 사용하는 컴퓨터로 교사용 PC, 노트북, 학생용 PC 등을 포함	PC, 노트북
물리적 자산	그 외의 자산으로 에어컨, UPS, AVR, 소화기 등과 같은 전산실 부대장비, 사무실, 전산실 부대설비 등과 같은 물리적 공간을 포함	부대시설, 물리적 설비, 경보시설

3.3 학내 정보자산의 보안성 평가

3.3.1 학내 정보자산의 평가 모델



(그림 2) 학내 정보자산의 평가 모델

3.3.2 학내 정보자산의 보안 항목 및 문제점

현재 중등학교는 초고속의 학내망으로 연동되어 있으며 NEIS를 통한 학생에 관한 교무/학사 등의 업무와 행정 자료 등이 개인 컴퓨터와 인터넷을 통한 서버에 저장되어 있다. 만약, 내부나 외부에서 데이터를 불법적으로 접근하여 데이터를 손실하거나 또는 NEIS 서버의 공격을 통해 데이터 이용을 방해할 경우 심각한 피해를 입을 수 있다. 다음은 학내 정보 자산의 분류에 따른 보안 항목과 보안의 문제점을 제시하였다.

<표 2 >

◆ **학내 정보자산의 분류에 따른 보안항목**

유형	보안 항목
네트워크	필터링, 로깅, 모니터링, 암호화 등
서버	취약점 보호, 접근제어, 사용자관리, 로그 분석, 저장매체 보호 등
PC	개인자료보호, 바이러스 탐지, 암호화 등
프로그램	사용자 식별, 사용 등급별 접근통제 등
물리적자산	전산센터 운영, 장비 보안, 재해 대책 등

< 표 3 >

◆ 정보자산의 분류에 따른 보안의 문제점

유형	문제점
네트워크	라우터 필터링은 가능하나 즉각적인 대처 미흡 로그 시스템 구현 암함, 모니터링 인원 부족 네트워크 상의 암호화 지원 안 함. 규모는 작으나 건물의 따라 산재되어 있음
서버	방화벽이 설치되어 있으나 서버의 취약점은 그대로 지니고 있음
PC	대부분의 PC 사용자의 보안 의식 부재
프로그램	관리자의 관리 소홀로 불필요하게 허용된 경우가 많음
물리적 자산	전산실 운영을 통해 해당 건물은 물리적 보안을 하는 경우가 많으나 그 외 건물에 있는 많은 장비에 대해서는 거의 물리적 보안이 안 되고 있음.

3.3.3 학내 정보자산의 보안 평가 지표

(1) 네트워크 자산의 평가

네트워크 레벨(IP, 포트, 프로토콜) 등에서 네트워크 자원의 조작을 통하여 일어날 수 있는 공격에 대한 방어를 하는 역할로 주로 방화벽으로 표현되어지는 하드웨어와 소프트웨어를 말한다.[8] 학내 전산망은 내부 네트워크와 외부 네트워크를 분리하여 내부 네트워크의 정보 자원을 불법적으로 접근하지 못하도록 하여 보안강화와 보안 통제를 주로 이용하고 있다.

< 표 4 > 네트워크 보안 평가 지표

평가지표	평가 항목
장애관리	장애 원인 규명 유지보수업체에 신속한 연락
구성관리	서로 다른 사설IP 대역을 사용
	논리적 네트워크영역으로 분리(VLAN)
보안관리	방화벽을 통한 접근 통제
	포트의 제어
	라우터의 접근제어 기능
	접속경로 통제
성능관리	트래픽 모니터링과 필터링
	불필요한 전자메일/파일전송(P2P) 상호 접속 통제

(2) 서버 자산의 평가

학내 전산망의 서버는 방화벽서버, 프락시 서버, 웹 서버, C/S 서버 등이 존재할 수 있는데 일반적으로 Unix 나 리눅스 계열의 운영체제(OS)를 사용하고 있다. 다음은 서버 자산의 평가 항목이다.

< 표 5 > 서버의 보안 평가 지표

평가지표	평가 항목
취약점 보호	OS와 시스템 소프트웨어의 Update 및 Patch
접근제어	접근제어 설정파일에 관리를 위한 IP에서만 접속가능
	접근제어설정파일 root만이 write
사용자 관리	불 필요한 서비스나 계정 삭제
	계정 패스워드의 할당
	패스워드의 암호화
	시스템의 중요한 설정파일들의 퍼미션 설정을 변경 (/etc/exports, /etc/fstab, /usr/bin/write, /bin/mount 등)
	관리자 계정(root)의 보안대책
로그 분석	사용자 ID, 로그온, 로그오프, 접속 시도 내용 등 모든 감시기록 유지
	주요정보 파일에 대한 내부자의 접근시 파일명, 파일내용, 사용자 ID, 일자 등을 기록
	모니터링 기록 주기적 검토
저장매체보호	서버의 중요내용의 확인 및 백업
서비스관리	/etc/inetd.conf 의 소유자가 root이며, 퍼미션이 644이하 유지
	불 필요한 ftp 서비스를 제거
	불 필요한 sendmail 서비스 제거
	서비스 접근 제한 (/etc/inetd.conf, etc/hosts.allow, /etc/hosts.deny 파일 수정)
	기타 불필요한 서비스(shell, rshd, rlogind, rexed 등)를 제거

(3) PC 자산의 평가 지표

학교 내의 자산 중에서 가장 많은 부분을 차지하는 것이 학내망에 연결된 PC 이다. 보안 지표로 제시할 수 있는 것은 다음과 같다.

< 표 6 > PC의 보안 평가 지표

관련지표	평가항목
개인정보 보호	중요한 데이터의 암호 지정
	공유폴더의 암호 지정
	부팅시 암호의 지정
	화면보호기 암호 지정
바이러스탐지	백신 설치

(4) 프로그램 자산의 평가 지표

학교 업무와 교수학습에 관련된 프로그램은 종류와 수량이 점점 많아지고 있으며 그에 따른 보안도 중요하게 생각되고 있다.

< 표 7 > 프로그램의 보안 평가 지표

평가지표	평가 항목
접근제어	사용자의 등급별 접근, 암호 사용, 도난 분실 주의

(5) 물리적 자산의 평가 지표

다른 정보자산을 보호하기 위한 넓은 범위의 자산으로 물리적인 접근통제가 중요하다.

< 표 8 > 물리적 자산의 보안 평가 지표

평가지표	평가 항목
접근제어	출입통제, 무인경비시스템 동작

4. 결 론

정보의 공유라는 특징을 지닌 인터넷의 급속한 성장과 함께 학교 내부의 정보 자산이 내부의 인가된 사용자 뿐 아니라 외부 침입자들에 의해 많은 위협을 받는 대상이 되었다. 현재 초·중·고의 학내 전산망은 보안상의 문제점으로 해커들의 불법 공격에 노출되어 학교 내의 각종 전산 자료가 쉽게 제3자에게 유출될 소지가 있다. 이에 따라 본 연구에서는 학교 내의 정보자산을 분류하였고, 네트워크, 서버시스템, 프로그램, 물리적 자산으로 분리해서 평가지표를 도출하여 정보보안의 개선에 초점을 두어 전개하였다. 보안의 중요성이 높아지고 있는 시대의 흐름에 따라 인터넷이라는 개방형 통신체제 속에서 학교 전산망 내의 모든 전자 문서들도 보안을 통한 정보 공유와 각 단위 학교 시스템의 보안 수준을 높이고 향후 행정정보시스템(NEIS)의 보안 수준도 강화될 것으로 기대된다.

참고문헌

[1] 유은종, "지식정보사회 이끌 인재양성에 주력", 정보화로 가는 길, 2000. 2.

[2] 강성준, "교육행정정보시스템(NEIS) 운영개선 방안에 관한 연구", 성균관대학교 교육대학원, 석사학위 청구논문, 2003. 4

[3] 이규복, "교육정보시스템을 위한 보안 및 요소기술에 관한 연구", 중주대학교 산업대학원, 석사학위 청구논문, 2003. 2

[4] 2003. 7. 7 일자 동아일보 기사 http://www.donga.com

[5] 교육부, 멀티미디어교육지원센터, 교육정보화 기반 구축 통합 모델 규격자료집, 1998

[6] 월간지 정보보호 21c, 2002. 8

[7] William Stallings, "컴퓨터 통신보안", 2001

[8] 박동석, "네트워크 보안성평가 지표개발에 관한 연구", 정보보증논문지 2002. 6

[9] 김연호, "지역망의 내부사용자 오남용에 대한 연구", 중부대학교 산업과학대학원, 석사학위 청구논문, 2000. 12

고 진 흥

1999년 광운대학교 제어계측공학과(공학사)

2004년 성균관대학교 교육대학원 컴퓨터 교육학과 (석사)예정

제1회 한국사이버테러정보전학회 춘계학술발표대회 (2004.5)

안 성 진
1988년 성균관대학교 정보공학과(공학사)
1990년 성균관대학교 대학원 정보공학과(공학석사)
1998년 성균관대학교 대학원 정보공학과(공학박사)
1990년 ~ 1995년 한국전자통신연구원 연구 전산망 개발실 연구원
1999년 ~ 현재 성균관대학교 컴퓨터교육과 조교수