정보보안 강화를 위한 K-water 사이버 보안센터 구축

이영우*, 오승엽
충남대학교 공과대학 전자공학과

K-water Cyber Security Center for Information Security Strengthening

Young-Woo Lee*, Seung-Hyueb Oh
Dept. of Electronic Engineering, ChungNam Univ.

Abstract - 곳곳에 산재한 컴퓨터를 시간과 장소에 상관없이 자유롭게 이용함으로써, 편리하고 쾌적한 정보이용환경을 구현하게 해주는 유비쿼터스 사회(Ubiquitous Society)는 동시에 예측 불가능한 위험이 곳곳에 산재한 '고도화된 정보위험사회'로의 진입을 의미한다. 본 논문에서는 인터넷을 통해 날로 지능화·고도화되는 사이버 위협으로부터 정보자산에 대한 안정성 강화와 분산 운영되는 보안관리 시스템(ESM)을 통합 모니터링하여 사이버위협상황에 대한 실시간 감시·대응을 체계적이고 효율적으로 수행하기 위한 K-water 사이버보안센터(Cyber Security Center, CSC)를 구축하였으며 이를 통한 신뢰성 있는 사이버보안체계를 제시하고자 한다.

1. 서 론

1.1 정보보안의 필요성

"정보보안"이란 일반적으로 보호해야 하는 정보자산을 명확히 한 후에 그 정보를 외부로부터의 공격이나 내부 유출 등으로부터 지키는 것을 말한다. 보다 구체적으로는 권한이 있는 자만이 정보에 접근할 수 있는 「기밀성(Confidentiality)」, 정보나 그 처리가 정확하고 완전한 「완전성(Integrity)」, 그리고 필요한 때에 확실히 정보를 접속할 수 있는 「가용성(Availability)」을 확보하는 것이다.[1]

위험사회(Risk Society)란 독일의 사회학자인 울리히 벡(Ulrich Beck)이 제시한 개념으로 과학기술의 발전으로 사회가 풍요로워질수록 예측 불가능한 위험이 증가하는 사회를 말한다. 정보위험사회(Information Risk Society)란 특히 컴퓨터와 네트워크와 같은 정보기술의 발전에 따라 대중들이 많은 혜택을 누리면서도 정보기술에 의해 등장한 다양한 역기능들과 같은 새로운 위험들에 노출되어 있는 사회를 말한다.

곳곳에 산재한 컴퓨터를 시간과 장소에 상관없이 자유롭게 이용함으로써, 편리하고 쾌적한 정보이용환경을 구현하게 해 주는 유비쿼터스 사회(Ubiquitous Society)는 동시에 예측 불가능한 위험이 곳곳에 산재한 '고도화된 정보위험사회'로의 진입을 의미한다. 특히, 유비쿼터스 사회의 근본 핵심기술이라고 할 수 있는 RFID, USN, VoIP, BcN, Wibro, Telematics 등의 잠재적 보안 취약성와 개인정보보호 침해 가능성은 다양한 잠재적 리스크들을 내포하고 있다.[2]

<표 1> 정보침해의 유형[3]

분류	예	설명
시스템	관리자 및 사용자 부주의	·추측이 쉬운 패스워드 사용 ·부주의한 시스템 신뢰관계 설정 ·사용자/퇴직자 미확인 또는 관리 부주의
	응용프로그램 버그	응용프로그램의 보안 관련 버그
	구성 오류	응용프로그램 구성상의 보안 관련 오류들
네트워크	구조적 취약점	프로토콜 설계상의 보안 취약점
	응용프로그램 버그	·네트워크 서비스 프로그램의 보안관련 버그들
	구성 오류	·네트워크 서비스 구성상의 보안관련 오류들

2003년 1월 25일, 슬래머웜에 의해 발생한 인터넷 대란을 계기로 사이버위협에 의한 국가안보 위기 가능성이 현실로 나타나자, 정부는 민·관·군을 일원화된 관리체계를 2004년 수립하였다. 또한, 2005년 1월에 국가사이버안전관리규정이 제정되어 국가안보를 위협하는 해킹 및 웜·바이러스 등 사이버공격으로부터 국가정보통신망을 보호하기 위한 체계적인 조직 및 운영방안이 마련되었다. 국내 관련 기구는 국가사이버안전센터, 국방정보전대응센터, 인터넷침해사고대응지원센터, 대검찰청 인터넷범죄수사센터, 경찰청 사이버테러대응센터, 국가보안기술연구소, 정보공유분석센터(ISAC)를 들 수 있다.

1.2 선진기관 정보보안 정책 소개

미국은 정보보안 정책 수립 및 집행을 위해 국가전략 수립, 법제도 정비, 사고대응체계 정비, 민관협력 강화 및 정보보호문화운동 추진 등의 5개 영역을 중심으로 관련 업무를 수행한다. 특히, 국가전략부문은 2002년에 발표된 국가안보 국가전략을 비롯하여, 국가 주요기반시설 및 주요자산에 대한 물리적 보호 전략, 사이버공간 보호를 위한 국가전략, 국가안보전략을 규정하고 있다.[4]

일본은 1996년부터 통산성·우정성·경찰청 등에서 개별적으로 사이버테러 방지를 위한 기술개발 및 정책연구를 추진했고, 1999년 8월에 공동 입안한 「부정 접속 행위의 금지 등에 관한 법률」이 국회를 통과함으로써 본격적으로 정보보안 활동이 시작되었다.[5]

영국은 정보통신 환경변화 및 이에 따른 정보보안 환경변화에 적극적으로 대처하고 있으며, 이에 따라 정보보안과 관련한 입법 활동이 비교적 활발한 국가 중 하나이다. 영국은 유럽연합의 기본적 정보보안 및 개인정보보호 조치들을 자국법으로 수용하는데 적극적이며, 미국 등 타 국가들이 주도적으로 추진하는 정보보안 정책들을 받아들이는 데에도 적극적이다.[6]

2. K-water 사이버보안센터 구축

2.1 사이버보안센터 개요

'03년 10월 공사 최초로 보안관제시스템(ESM) 구축 계획 수립을 시작으로, '04년 경영정보망(OA), '05년 로그분석시스템, 발전통합망(GIOS)의 보안관제시스템(ESM)이 구축 완료되었으나, 각 부서별로 발생되는 보안관련 정보 공유가 원활하지 않아 통합 감시, 종합적 보안현황 분석, 운영정보 공유 등의 어려움이 발생되었다. 또한, 2006년도 공공분야 사이버 침해사고 발생 건수가 4,286건으로 집계되어 사이버테러의 위험 증가와 대처방안 마련이 시급하였다.

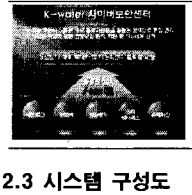
<표 2> 2006년 공공분야 침해사고 발생 현황 (출처 : 2007 국가정보보호백서)

유 형	악성코드 감염	경유지 악용	홈페이지 변조	자료훼손 및 유출	기 타	합 계
국가기관	316	59	16	49	16	456
공공기관	2,232	1,257	237	74	30	3,812
합 계	2,548	1,316	253	123	46	4,286

이에 따라, 한국수자원공사는K-water 정보망을 실시간 통합관제 할 수 있는 사이버보안센터(K-water Cyber Security Center, K-water CSC)를 구축하였다.

분산되어 운영 중인 ESM을 중앙집중적으로 통합하여 시스템별 정보를 유기적으로 수집 및 종합적인 분석결과를 토대로 사이버위협으로부터 공동 대응할 수 있는 통합관제체계를 구축함에 따라, IT 서비스 질 향상을 통한 디지털 경영체계 보호기반 마련하고, 보안시스템의 최적화 관리를 통한 효율성을 증대시키고, 종합적이고 일관성 있는 보안정책관리와 사이버침해 사전대응할 수 있으며, 국정원과 상호공조체계 구현으로 위기대응체계 확립 등의 효과를 기대할 수 있다.

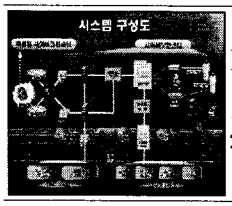
2.2 운영방향



K-water CSC는 침입방지, 방화벽 등 각종 보안시스템 및 주요 정보자원들을 일괄된 정책으로 통합관리하고 사이버 위협에 대한 정보수집·분석, 차단 및 사고대응 강화를 통해 정보보안 체계 극대화와 안정적인 네트워크 운영을 목표로 하고 있다.

2.3 시스템 구성도

로깅 및 분석된 정보들은 인터넷망을 통하여 국정원 사이버안전센터에 실시간 전송함으로써, 전사적 사이버 위협에 대한 공동분석 및 조기대응 체계가 가능하도록 구성하였다.



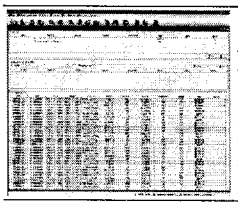
침입차단·방지·탐지 시스템, 통합 바이러스 관제시스템, 유해사이트 차단 시스템 등 총 10종의 정보보안 시스템 172대를 운영 중에 있다. 인터넷망을 통해 송수신되는 정보들은 1차적으로 바이러스월을 거쳐 2차 방화벽, 3차 침입방지 시스템으로 필터링 되면서 악성코드, 웜·바이러스에 대한 대응을 실시하고 있다.

2.4 관제 운영 절차

사이버보안센터는 관제요원 2인이 통합보안관제시스템(TSM)을 통해 경영정보망, 수도통합망, 발전통합망 및 댐통합망의 ESM을 실시간 모니터링함으로써, 실시간 위험요소를 분석하고 각 시스템 담당자에게 위험 경보를 발령 등 유기적인 공조체계를 구축하였다.

3. 주요 시스템 기능 및 운영 결과 분석

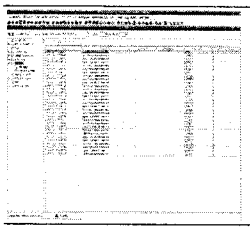
3.1 통합보안관제시스템(TSM)



침입방지시스템(IPS) 등의 각종 정보보호시스템의 로그 이벤트를 종합 분석하여 실시간 대응과 관제대상 장비들의 현황 및 장애관리가 가능하다. 필터링/레벨화를 거친 이벤트와 트래픽, 패킷, 시스템 부하 등 시스템 상태정보에 대하여 관리자에게 실시간으로 전달함으로 상호관계를 자동으로 분석할 수 있다.

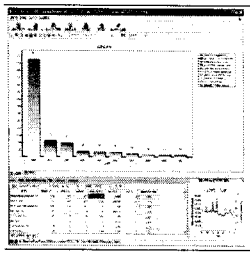
또한, 불법 정보 유입을 막기 위해서 등록된 관제대상 장비로부터 오는 데이터만을 처리한다. 해커들이 특정 포트에 대한 과다한 트래픽 부하를 유발시키려는 시도가 있을 경우 해당 포트에 대한 방화벽 등의 정책설정을 통해 허용된 대역으로부터의 송신이 이루어짐에 따라, 정규화된 순수 이벤트 정보만 송수신하게 된다.

3.2 침입차단시스템(FireWall)



외부의 사용포트, IP에 대해 개별 보안정책을 설정함으로써 철저하게 Rule Base로 움직이고 있다. 관리자설정, IP 설정, 가상 IP설정, 네트워크 인터페이스, 라우팅 설정 등의 하위 메뉴를 가지며, 인터넷에서 사용이 허가되지 않은 비공인 IP 주소와 제한된 공인 IP 주소로 인터넷 접속을 할 수 있는 NAT기능을 제공한다.

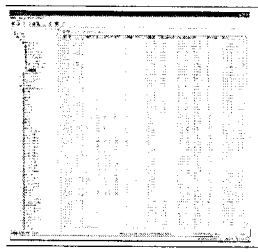
3.3 침입방지시스템(IPS, Intrusion Prevention System)



시스템 및 네트워크 자원에 대한 다양한 침입행위를 즉각적으로 탐지하고 분석하여 비정상으로 판단된 패킷을 차단시키고 의심스러운 세션들을 종료시킴으로써 공격에 능동적으로 대응하는 기능을 하고 있다. 서비스거부(DoS) 및 분산서비스거부(DDoS) 공격의 근본적인 차단과 방화벽이나 침입탐지시스템(IDS)에서 차단할 수 없는 사이버 공격에 대해 유동적인 방어가 가능하다.

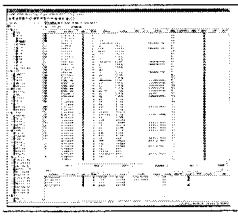
또한, 악의적 행위에 대한 실시간 자동차단(Drop)으로 네트워크 관리의 효율성을 증대시키며, 잠재위협에 대한 탐지 및 방어, 관리(Threat Management System)가 가능하여 네트워크 및 시스템에 대한 통합보안정책 수립이 가능하다.

3.4 보안운영체계(SecureOS)



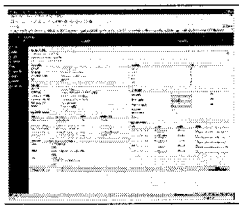
외부 해킹, 내부자 보안범죄 등 주요 서버에 대한 다양한 형태의 위협을 방지하기 위한 운영체계로 강력한 보안기능을 수행하며, 서버의 정보자산에 대한 불법적인 위·변조 및 탈취를 차단하는 보안기능을 위하여 다중등급보안, 강제적 접근제어 등을 수행한다.
사이버 공격의 유형에 관계없이 원천적으로 해킹을 차단할 수 있는 기반을 제공하며, 자기 자신을 외부의 공격으로부터 보호하고 있다.

3.5 IP관리 시스템(IPKeeper)



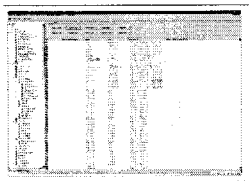
네트워크 자원의 자동 수집관리, IP충돌 방지, 네트워크 사용률 모니터링/사용 History 관리, IP와 MAC간의 고정기능으로 특정 IP사용의 원천봉쇄 등 네트워크 관리 기능이 있다. 또한, 인증되지 않은 IP/MAC 장비의 네트워크 사용 차단, 각 장비간의 통신의 제한 기능, 각 장비들의 내부/외부 통신망 접근 제한 등 내부 보안 관리 기능이 있다.

3.6 바이러스 월(Virus Wall)



네트워크 경계지점에서 네트워크를 통해 유입되는 컨텐츠의 바이러스 감염여부를 검색하고 차단해 바이러스의 확산과 그로인한 피해를 최소화하고 HTTP, FTP 등과 같은 다양한 프로토콜에 대한 검사 기능을 수행한다. 네트워크 구간에 인라인(In-Line)방식으로 설치·운영되기 때문에 네트워크 환경 변경 등 별도의 수정이 필요 없다.

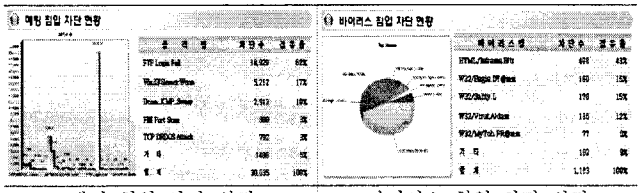
3.7 유해사이트차단시스템



공사 내부의 컴퓨터를 사용해서 누가 어느 사이트에 접속하고 있는지에 대한 전체 상황을 실시간 모니터링 및 통계처리하고 개인/그룹/전체를 대상으로 유해사이트에 대한 다양한 차단/관리 정책을 설정할 수 있다. 다양한 형태의 보고서 작성 기능이 있어, 내부보고 시 기능 그대로 활용되고 있다.

3.8 운영 결과 분석

사이버 보안센터의 운영은 주 단위로 공사 내 OASIS 게시판을 통하여 사용자에게 공유함으로써, 네트워크의 해킹침입 및 바이러스 위협에 대한 사용자의 인식 제고를 근간으로 하고 있다. 한 달 동안 운영한 사이버 보안센터의 운영결과는 39,583건의 해킹침입과 9,834건의 바이러스를 차단함으로써, 전사적 피해확산을 사전 방지하였음을 알 수 있다.



해킹 침입 차단 실적 | 바이러스 침입 차단 실적

4. 결 론

본 연구에서는 K-water 사이버보안센터(Cyber Security Center, CSC)의 구축을 통하여 신뢰성 있는 사이버 보안체계를 제시하고, 사이버 해킹 및 바이러스 침입에 대한 차단 효과를 분석하였다. 이를 통하여 인터넷을 통해 날로 지능화·고도화되는 사이버 위협으로부터 정보자산에 대한 안정성 강화와 저·실별 분산 운영되는 보안관리시스템(ESM)을 통합 모니터링하여 사이버위협상황에 대한 실시간 감시·대응을 체계적이고 효율적으로 수행할 수 있도록 시스템화 하였다. 또한 인터넷 웜, 바이러스 해킹 등의 사이버공격에 대한 침입탐지, 트래픽 및 상관관계 분석을 통해 종합적인 위협분석 및 글로벌 위협, 취약성 정보, 조기 예·경보 전송 및 실시간 대응을 통해 사이버 위협의 관제 및 조기 대응체계가 확립될 것으로 기대된다.

[참 고 문 헌]

[1] 국가보안기술연구소, "일본의 新 정보보안 체계 구축 동향II", 2006.12
[2] 조차석, "정보사회에서의 정보보안에 관한 연구", 한국문헌정보학회지, 제34권 제1호, pp 155~180, 2000.3
[3] 임종인, "정보사회의 통합적 위협관리 기술로의 정보보호 패러다임 변화", 사이버시큐리티 1월호, 2008.1
[4] 국가보안기술연구소, "미국의 정보보안 관련 법제도 소개", 사이버시큐리티 4월호, 2007.4
[5] 국가보안기술연구소, "일본의 정보보안 관련 법제도 소개", 사이버시큐리티 5월호, 2007.5
[6] 한국전자통신연구원, "영국의 정보보안 관련 법제도 소개", 사이버시큐리티 10월호, 2007.10