2007년도 대한전기학회 전력기술부문회 추계학술대회 논문집 (2007. 11. 2 ~ 3)

우리나라 전력계통의 사이버테러 대응방안 고찰

강 순 희, 손 윤 태, 김 성 학
한국전력거래소

Response plan against cyber terror on Korean electricity sector

Kang Sun-Hee, Sohn Yoon-Tae, Kim Sung-Hak
KOREA POWER EXCHANGE Information Technology Department IT Planning & Operation Team

Abstract - 전력계통 보안관제센터는 전력IT의 사이버테러 위험을 줄이고 보안을 강화하는 것이다. 이를 위해 전력산업 관계기관은 해킹·바이러스와 같은 사이버공격에 대한 대응을 고도화하기 위해 전력거래소 내 전력계통보안관제센터(ES-ISAC)에 실시간 관제·대응센터를 만들고 시스템 성능의 지속적인 업그레이드 작업과 다른 시스템과의 연동을 확대함으로써 사이버침해 사고에 대한 예측력을 향상시키는 작업을 추진해야 한다. 침입기술, 웜·바이러스 샘플 분석과 같이 침해사고 정보수집을 보다 능동적으로 하고 모든 정보에 대한 백업시스템을 구축함으로써 안정적인 센터운영을 기해야 한다.

1. 서 론

연구와 군사 목적으로 발전한 인터넷은 현재 많은 기업들과 일반인들이 사용하게 되었고 현대 사회에서 중요한 기반으로 에너지, 교통통제, 항공관제 등 제어시스템까지 제어하는 수단으로 자리 잡게 되었다. 더구나 우리 일상생활에서 없어서는 안되는 전기가 발전소에서 가정까지 공급되기 위해서는 수많은 전력시스템이 전력IT에 의해 제어된다는 사실을 아는 사람은 그리 많지 않을 것이다. IT기술의 급진전으로 전력산업의 IT의 의존도는 날이 갈수록 증가하여 전년도 전력시장운영시스템을 통한 경제급전 운영으로 연간 1200억의 연료비를 절감 전력산업의 효율성 제고에 전력IT가 크게 기여하고 있다.

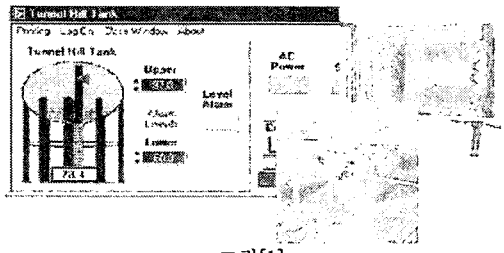
그러나 IT기술 발전만큼 역기능으로 인한 보안문제가 전력IT에 미치는 영향이 커짐에 따라 보다 많은 관계자들은 정교해진 공격용 프로그램에 대응할 방안은 없는지 고심하고 있는 것이다. 악의적인 목적을 가진자에 의해 전력IT가 해킹 또는 웜바이러스로부터 침해되었을 경우 2003년 1.25 인터넷 대란과 같은 전력대란을 경험하게 될지도 모른다. 산업현장, 병원, 학교, 가정 등 모든 분야가 전력공급이 한순간이라도 중단되어선 안되는 곳이다. 본고에서는 이러한 초유에 사태를 예방할 수 있는 방안은 없는지 논의해 보고자 한다.

2. 본 론

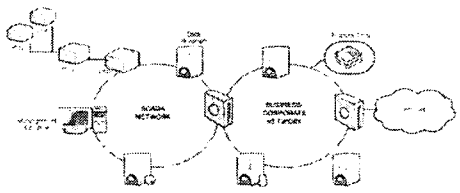
2.1 전력IT 개방성과 확장성

전력과 같이 대규모 플랜트를 운영하기 위해서 필수적으로 사용되는 시스템은 센서, 제어계통, 통신망 및 컴퓨터로 그림[1]과 같이 구성되어 있다. 즉 원방감시제어시스템(Supervisory Control And Data Acquisition) 분산제어시스템(DCS : Distribution Control System), 공정제어시스템(PCS : Process Control System) 등이다.

이러한 시스템 환경의 특징은 해킹 및 웜바이러스 등에 쉽게 노출될 수 있는 네트워크 및 시스템의 취약성으로 인하여 침해속도가 매우 빠르게 진행되어 "15분의 전쟁"이라고 이야기될 정도로 급격하게 전파되는 피해속도에 있다. 그 원인은 바로 이러한 전력IT 네트워크의 개방성과 확장성에 있다. 본래 인터넷은 개방형 프로토콜로 개발되었으며 네트워크 성능향상을 위한 멀티캐스트 등의 기법을 이용하고 있으나 이러한 개방성과 확장성은 그림[2]와 같이 서로 다른 네트워크가 통합되어 보안과는 상반되는 특징을 가지고 있다.



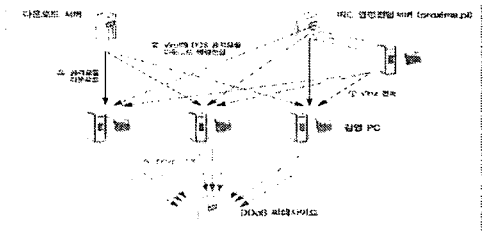
그림[1]



그림[2]

2.2 다양한 공격형태와 현황

네트워크의 취약점을 통한 공격방법이 점차 복잡해져 백신이나 침입탐지시스템을 이용하여 공격의 흔적을 찾기가 점점 어려워지고 있으며 그림[3]과 같이 분산서비스 거부공격(DDoS)이 다양한 공격형태와 결합하면서 엄청난 피해를 야기하고 있다.



그림[3]

지난 '03년 1월 25일의 인터넷 침해사고와 일련의 인터넷 침해사고를 보면 전력IT의 가용성(Availability)에 중대한 영향을 줄 수 있는 인터넷 웜(Internet Worm)에 의한 공격이 일반화되고 있음을 알 수 있다. 그림[4]와 같이 한국정보보호진흥원(KISA)의 통계에 의하면 자가복제, 고속전파, 서비스 거부 등의 성격을 가진 인터넷웜은 매월 450여건씩, 에이전트화, 분산화, 자동화의 특징을 지닌 악성 봇(Bot)은 전체 해킹 건수의 11%이다 최근 공격의 형태를 보면 사용자 단말기가 분산서비스 공격을 위한 Agent로 악용되고 있다는 것이다.

침해사고 전체 통계

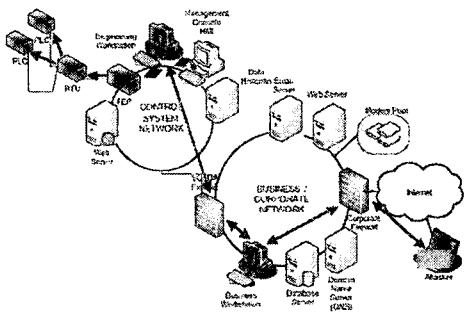
구분	2006	2007												2007
	총계	1	2	3	4	5	6	7	8	9	10	11	12	총계
웜·바이러스	7,789	518	622	329	395	309	422	424	411	559				3,989
정보삭제형	26,908	2,156	2,169	2,247	2,220	1,966	1,541	1,931	1,950	1,445				17,627
• 서종대비	14,055	1,225	1,473	1,477	1,310	972	477	851	1,248	677				9,710
• 파일감염	1,266	90	170	96	73	90	68	79	78	92				846
• 단순스캔수	3,711	327	184	414	536	522	476	315	317	243				3,336
• 기타형	4,570	229	206	197	212	217	213	201	182	197				1,854
• 정보제형	3,206	287	148	63	69	145	305	485	125	236				1,883
악성 봇(Bot)	12.5%	13.7%	13.0%	11.9%	11.6%	10.8%	10.2%	10.1%	9.4%	11.4%				11.3%

그림[4]

지난 2003년 8월 블래스터(Balster)와 웰치아(Welchia), 소빅F웜(Sobig.F) 등 바이러스 공격으로 전세계적으로 한 달 동안의 경제적 피해규모가 328억불에 달한다.

2.3 전력IT의 취약성

일부 전력분야의 보안전문가는 전력IT가 폐쇄망이기 때문에 안전하다는 견해들이 있기는 하지만 최근 전력IT의 환경은 매우 취약한 상태로 진전되고 있다는 사실이다. 대부분의 전력관련 경영진은 전력IT 네트워크가 ERP 등과 연결이 안된 것으로 인식하고 있으나 보안기관의 측정결과 대부분 전력IT가 그림[5]과 같이 내부시스템과 연결된 것으로 파악되었다.



그림[5]

이와 같이 전력산업도 효율성 제고, 정보공개의 확대 등 제어시스템의 실시간 운영정보 확보가 필요하면서 인트라넷, 상용망과 상호연계는 필요불가분의 관계가 되어버렸다. 보안상 취약하기 때문에 시대적 욕구를 저버릴 수는 없는 상황에 와 있는 것이다. 사실을 은폐하는 것은 보다 사실에 입각해서 근본적 대책이 필요한 시대이다.

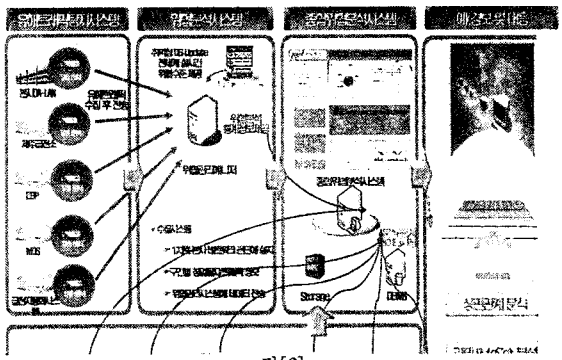
2.4 전력IT의 침해사례

해외 전력IT 침해사례를 보면 2003년 1월 25일 슬래머웜에 의해 오하이오 Davis-Besse 원자력발전소 안전모니터링 시스템이 5시간 동안 중단되었고, 알카에다 교육훈련소의 컴퓨터에 사이버테러가 가능한 댐과 관련된 전력IT 정보가 발견되었고, 유럽의 배전시스템 내에 패치가 되지않은 시스템과 라우터에 웬치아 웜이 유포되어 전력IT 관련 통신시스템의 30~40%가 마비되는 등 다수의 피해가 발생했다.

우리나라의 경우 전력IT의 보안성 확보를 위해 보안시스템 도입 등 꾸준한 보안대책 수립 및 시행으로 이렇다할만한 피해가 없었지만 취약점을 통한 침해가능성은 항상 상존하고 있다 정부기관, 공공기관의 위협정보를 국가사이버안전센터가 관제 및 대응하고 있기는 하나 중요 전력IT까지 미치기엔 한계가 있다. 미국은 국토안보부 산하 전력계통 신뢰도협의회(NERC)에 ES-ISAC을 설치 사이테러의 위협정보를 실시간으로 공유하고 대응하고 있으며, 특히 정보보안 가이드라인(보안표준1300)을 제정 운영하는 등 전자적 침해사고에 대비해 보안활동을 더욱 강화하고 있다는 사실을 우리는 인식할 필요가 있다.

2.5 사이버테러 방지 방안

첫째, 현재 사용하고 있는 전력IT 네트워크의 위험을 줄이고 보안을 강화하는 것이다. 이를 위해 전력산업 관계기관은 해킹·바이러스와 같은 사이버공격에 대한 대응을 고도화하기 위해 전력계통도 보안관제센터(ES-ISAC)에 실시간 관제·대응센터를 만들고 시스템 성능의 지속적인 업그레이드작업과 다른 시스템과의 연동을 확대함으로써 사이버침해 사고에 대한 예측력을 향상시키는 작업을 추진해야 한다. 침입기술, 웜·바이러스 샘플 분석과 같이 침해사고 정보수집을 보다 능동적으로 하고 모든 정보에 대한 백업시스템을 구축함으로써 안정적인 센터운영을 기해야 한다. 그림[6]은 일반적인 ISAC의 구성도로서 탐지시스템, 위협분석시스템 및 종합분석시스템으로 구성되어 있다.



그림[6]

또한 국가사이버안전센터 및 에너지보안관제센터 등 방역센터를 확대 운영하으로써 주요 운영체제의 패치서비스를 제공하고 [redacted] 인터넷침해사고 대응팀 CERT를 활성화하며 정보공유 및 분석센터(ISAC)의 지원을 강화함으로써 국내에 고도화된 정보공유체계를 빠른 시일내에 구축함으로써 한차원 높은 정보보호 환경을 기대할 수 있을 것이다.

둘째, 인터넷의 구조적 문제를 기술적으로 보완해 나가야 한다. 인터넷 기반구조 보호를 위한 고도화된 정보보호기술의 표준화를 추진하고 국내·국제 표준화를 추진하며 IPv6용 정보보호기술을 개발하고 안전한 시스템 운영을 위한 Secure OS를 개발하는 등 기반구조 보호를 위한 기술개발에 노력을 기울여야 한다. 그리고 침입에 대한 탐지·대응 등의 기능을 수행할 수 있는 Secure 엔진과 이를 탑재한 Secure 노드 등으로 구성된 차세대 네트워크 정보보호 기술개발을 함께 진행하여야 한다.

세째, 정보보호를 위한 국가기관·공기업간의 협조체제를 공고히 하고 해외와 정보공유를 위한 긴밀한 관계를

유지하는 것이다. 해외 정부 및 침해사고대응기관, 국제단체 등과 실질적인 공조체제를 구축하고 침해사고 발생시 상황전파, 대응현황 등의 정보를 공유함으로써 높은 전력IT 정보보호의 위상을 보여줄 수 있는 것이다.

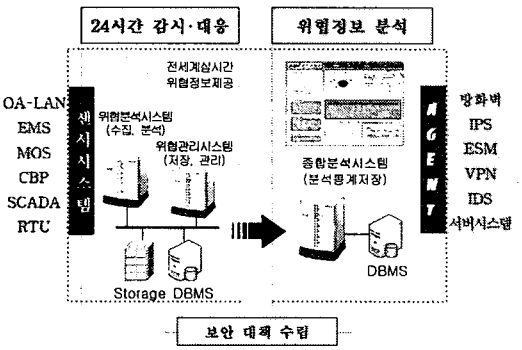
2.6 전력계통 보안관제센터 구축

지난 2003년 8월 14일 미국 북동부와 캐나다 동부지역을 암흑으로 몰아넣었던 대규모 정전사태를 조사했던 북미전력신뢰도협의회(NERC)의 최종보고서에서는 "보안관련 정보와 분석결과를 전력회사간에 상호 관련정보를 공유하기 위하여 미국에서 운영중인 전력계통분야 정보공유분석센터 역할을 확립할 것"을 권고하였다.

우리나라도 전력계통에 대한 사이버테러 방지를 위하여 주요 전력IT의 전자적 침해행위를 사전에 인지, 발생가능한 위협에 적극적으로 대응하기 위한 "전력계통 정보공유분석센터 설립"의 필요성이 정부차원에서 제기 되었다. 이에 따라 전력계통을 실시간 제어하고 운영하는 전력거래소에서는 전력계통 보안관제센터의 역할을 수행하기 위하여 2007년도에 ISAC 운영을 위한 기반시설을 구축할 예정이다. 우선적으로 급전자동화설비(EMS), 시장운영시스템(MOS), 변동비방영시장운영시스템(CBP) 등 대표적인 전력IT설비와 OA 설비를 대상으로 실시간 사이버 감시체계를 구축하고, 향후 회원사의 전력IT설비로 보안관제서비스를 확대해 나갈 예정이다.

전력계통 보안관제센터의 주요 역할은 전력IT 설비에 대한 사이버 위협을 24시간 실시간으로 감시·대응하고 위협정보 분석을 통하여 취약점을 제거하며, 위협정보를 상위기관 및 전력그룹사에 신속히 전파되도록 하여 안전대책을 강구하는 등 정보보호에 공동으로 대처할 수 있도록 한다.

전력계통 보안관제센터의 구성은 그림[7]과 같이 네트워크의 유해트래픽을 수집하기 위한 센서시스템, 외부에서 유입되는 바이러스 등에 대응하여 의사결정 수단 제공하는 위협관리시스템, 보안설비에 설치된 에이전트로부터 수집한 정보를 종합적으로 분석하는 종합분석시스템으로 구성된다.



그림[7]

3. 결 론

정보통신기술의 발달로 전력산업에도 제어설비들의 광역화 및 네트워크화는 거스를 수 없는 시대의 대세이므로 전자적 침해에 노출될 수 밖에 없는 실정이다. 그러나 전력설비와 같은 국가 기간설비는 어떠한 상황에서도 사이버 테러에 방치되게 해서는 안 된다.

2003년도 인터넷 대란에서 경험했듯이 인터넷이 더 이상 가상의 네트워크가 아니라는 것을 여실히 보여줬으며, 이미 우리생활의 일부가 되어버린 인터넷의 실체를 되짚어 보는 계기가 되었다. 거미줄처럼 엮여있는 무수한 전력IT설비의 네트워크 중 어느 한 곳이라도 보안상 허점이 생긴다면 그것이 전력계통의 안정운영에 영향을 끼치게 되어 순식간에 정전으로 연결되어 국가안보까지 위협할 수 있는 대재앙으로 이어질 수 있다.

이런 의미에서 국가 경제발전과 국민생활에 필수적인 전력을 안정적으로 공급하기 위해서는 사이버테러에 대한 적극적이고 진취적인 자세로 대응해 나가야 하며, 아울러 취약한 정보보호 전문가를 적극 육성하여 전력계통의 사이버 파수꾼으로 역할을 할 수 있는 여건을 조성해야 한다.

[참 고 문 헌]

[1] 국가보안기술연구수, 제어시스템 사이버보안 동향, 이철원
[2] 에너지분야 내의 컨트롤시스템 보안을 위한 로드맵 에너제틱스 인코퍼레이티드
[3] 월별 사이버침해동향 정보보호대응반, 한국정보보호진흥원(KISA)